

(IN) SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 37 - March 2013

**PENETRATING AND ACHIEVING PERSISTENCE
IN HIGHLY SECURED NETWORKS**



**REVIEW
NIPPER
STUDIO**



**BECOMING A
MALWARE ANALYST**



**RSA
CONFERENCE
2013**

**APPLICATION SECURITY
TESTING FOR AJAX AND JSON**



**FIVE QUESTIONS FOR
MICROSOFT'S CHIEF
PRIVACY OFFICER**

SECURITY AWARENESS FOR THE 21st CENTURY

- Go beyond compliance and focus on changing behaviors.

- Create your own program by choosing from 30 different training modules.

- Meets requirements of the Data Protection Act and PCI DSS.

- Training is mapped against the 20 Critical Control framework.

- For more information visit us at www.securingthehuman.eu



www.securingthehuman.eu

TABLE OF CONTENTS

Page 05 - **Security world**

Page 13 - Becoming a malware analyst

Page 18 - Review: Nipper Studio

Page 21 - Five questions for Microsoft's Chief Privacy Officer

Page 24 - Application security testing for AJAX and JSON

Page 29 - **Malware world**

Page 33 - Penetrating and achieving persistence in highly secured networks

Page 38 - Report: RSA Conference 2013

Page 44 - Social engineering: An underestimated danger

Page 49 - Review: Hacking Web Apps

Page 52 - Improving information security with one simple question

Page 54 - **Events around the world**

Page 55 - Security needs to be handled at the top

Page 59 - 8 key data privacy considerations when moving servers to the public cloud

Welcome to (IN)SECURE 37 the digital security magazine



I recently got back from San Francisco where I attended RSA Conference 2013. Despite this being one of the busiest weeks of the year for me, nothing could prepare me for the massive expo that, for the first time, had to expand to a new space. 24,000 attendees and 360 exhibitors are an indication of massive growth and further position the information security industry as one of the best to have a career in.

Besides coverage from the conference, this issue goes behind the scenes of the anti-malware industry, teaches about the dangers of social engineering, offers tips for making our industry better, and much more. Enjoy!

Mirko Zorz
Editor in Chief

Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

Feedback and contributions: Mirko Zorz, Editor in Chief - mzorz@net-security.org
News: Zeljka Zorz, Managing Editor - zzorz@net-security.org
Marketing: Berislav Kucan, Director of Operations - bkucan@net-security.org

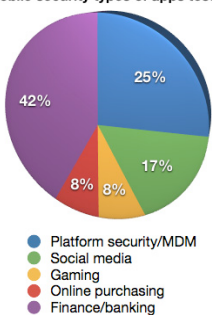
Distribution

(IN)SECURE Magazine can be freely distributed in the form of the original, non-modified PDF document. Distribution of modified versions of (IN)SECURE Magazine content is prohibited without the explicit permission from the editor.



Highlights from 450 global data breach investigations

Mobile security types of apps tested



Trustwave released details from a report that highlights details and trends from 450 global data breach investigations, 2,500 penetration tests, nine million Web application attacks, two million network and vulnerability scans, five million

malicious websites, 20 billion e-mails as well as research and analysis of zero-day security threats. Key findings:

- Applications emerged as the most popular attack vector.
- 64 percent of organizations attacked took more than 90 days to detect an intrusion with the average time for detection being 210 days -- 35 days longer than in 2011.

- Employees leave the door open to further attacks. Whether due to lack of education or policy enforcement, employees pick weak passwords, click on phishing links and share company information on social and public platforms.

- Attacks were discovered in 29 different countries. The largest percentage, 34.4 percent, originated in Romania.

- Spam volume shrank in 2012 but still represents 75.2% percent of a typical organization's inbound e-mail and roughly 10 percent of spam messages are malicious.

- Businesses seem to be rapidly adopting an outsourced, third-party information technology operations model.

- The two most noteworthy methods of intrusion, SQL injection and remote access, made up 73 percent of the infiltration methods used by criminals in 2012.

- Out of the 450 cases investigated in 2012, about 40 variations of malware were found, attributed to six criminal groups. Three criminal teams caused the majority of payment of service credit card breaches.

Bit9 hacked, its certificates stolen and used to sign malware



Bit9, a security firm that provides software reputation, application control and whitelisting services to companies in the financial, technology, government and other sectors, has announced that

it has suffered a breach that resulted in three of its customers to be infected with malware.

"Due to an operational oversight within Bit9, we failed to install our own product on a handful of computers within our network. As a result, a malicious third party was able to illegally gain temporary access to one of our digital code-signing certificates that they then used to illegitimately sign malware," explained Bit9's Patrick Morley.

"There is no indication that this was the result of an issue with our product. Our investigation also shows that our product was not compromised. We simply did not follow the best practices we recommend to our customers by making certain our product was

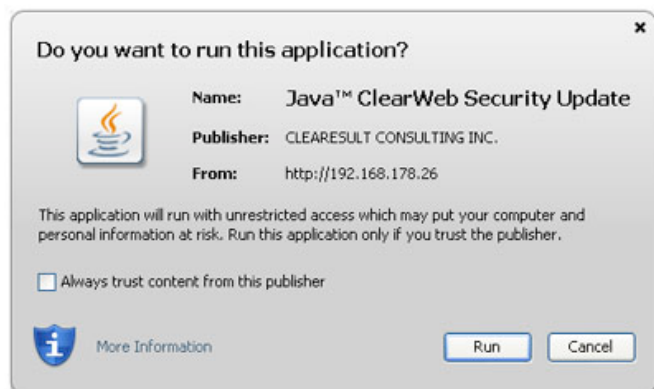
on all physical and virtual machines within Bit9."

The company reacted by revoking the affected certificate, making sure that Bit9 is installed on all of its physical and virtual machines, and will be issuing a patch for its software that will automatically detect and stop the execution of any malware that illegitimately uses the compromised certificate.

Bit9 has been touting its whitelisting approach as the right solution for blocking targeted attacks with specially made malware, which is rarely stopped by anti-virus solutions currently offered on the market. Unfortunately for them, it has now been proven that every approach - even theirs - has weaknesses.

If this successful attack has shown anything, is that there is no one solution that will be effective against all threats, and that a multilayer approach to defense is a must in the current threat landscape. It has also proven that even if you might consider your defenses to be adequate, those of your partners and collaborators might not be and can provide a wide enough hole in your perimeter to allow the attackers in.

Malicious Java applet uses stolen certificate to run automatically



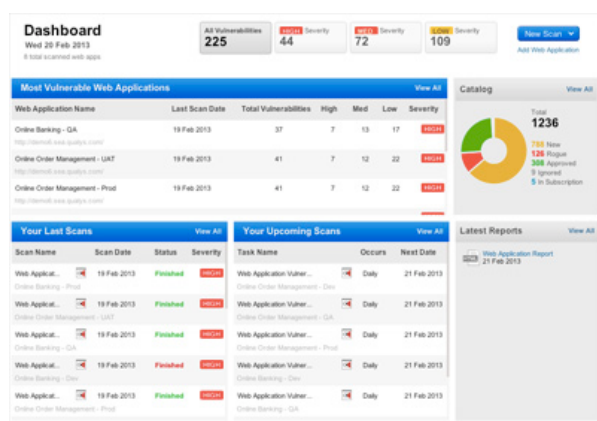
A signed but malicious applet that will apparently fool even the latest Java 6 update has been discovered on a German online dictionary website infected by the g01pack exploit kit, warned security researcher and Metasploit contributor Eric Romang.

The applet is signed with a stolen private key belonging to Texas-based Clearesult Consulting.

The certificate associated with the applet has been revoked late last year. Nevertheless, Java detects the applet as trusted and its default high security level doesn't automatically block it from running. Romang pointed out that signing and verifying files is a so important part of the Java platform's security architecture that Jarsigner validates the file despite the certificate having been revoked.

Jindrich Kubec, Director of Threat Intelligence at Avast, discovered the reason: Java has the "Check certificates for revocation" option turned OFF, and the "Enable granting elevated access to selfsigned apps" feature turned ON by default.

QualysGuard WAS 3.0 adds customers automation, accuracy and ease-of-use



Qualys released QualysGuard WAS 3.0, adding malware detection and attack proxy support to provide customers and consultants with comprehensive web application security testing. With this new release organizations can discover and catalog web applications on a global scale, then identify and remediate web applications vulnerabilities accurately and cost-effectively.

QualysGuard WAS 3.0 provides malware detection for web sites, using advanced behavioral analysis to identify even zero-day malware that may infect users. The service proactively scans web sites for malware, providing automated alerts and in-depth reporting to enable prompt identification and resolution of vulnerabilities.

Additionally, 3.0 introduces advanced scanning configurations and reporting enhancements including report creation wizard and scorecard reports based on asset groups or tags, making it easy for users to create and customize reports for the audience they are targeting.

QualysGuard WAS 3.0 enables organizations to integrate the scan results of attack proxies such as Burp Suite with its automated scans, presenting comprehensive reports of the results, giving organizations a complete view of vulnerabilities across their web applications.

Visit www.qualys.com/was for more information.

Microsoft also victim of recent watering hole attack



Microsoft has followed in the steps of Twitter, Facebook and Apple, and has confirmed that it has recently experienced a security intrusion.

"During our investigation, we found a small number of computers, including some in our Mac business unit, that were infected by malicious software using techniques similar to

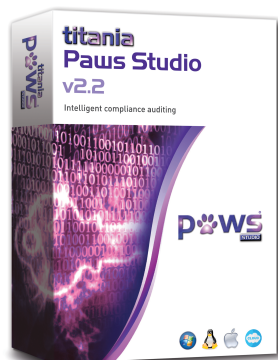
those documented by other organizations," stated Matt Thomlinson, General Manager of Microsoft's Trustworthy Computing Security, and added that so far, they have found no evidence of customer data being affected, but that the investigation is still ongoing.

Twitter, Facebook and Apple have recently notified the public about the breaches into their internal networks, which were the result of a watering hole-type of attack.

The watering hole in question was the iPhoneDevSDK forum site, popular with mobile developers, and the attacker have managed to infect the visitors' computer by serving exploits for (at the time unpatched) Java vulnerabilities.

It is still unknown whether the attack was aimed at these high-profile targets, but what is known is that it wasn't limited to them - any visitor that still had Java enabled on his browser or computer was bound to be affected.

Paws Studio: The compliance auditing tool for workstations and servers



Paws Studio is a compliance auditing tool that enables organizations to produce thorough and easy to action compliance audit reports on their windows based workstations and servers.

The reports can be generated in seconds using either the integrated pre-defined policies for various top computer usage standards, or by using the Paws Definition Editor to customize your own policy.

With Paws Studio you can:

1. Produce remote compliance audits using remote connectivity or audit offline with our unique Data Collector
2. Produce comprehensive reports and management summaries to appeal to all levels of your organization
3. Audit against pre-defined policies such as PCI, NSA, STIGS, SANS and NERC.
4. Create and modify your own policies using the Paws Definition Editor
5. Use the Remedy Table to quickly solve potential compliance issues
6. Script your audits so that can be written into your existing processes
7. Export into PDF, CSV, XML and HTML
8. Run multiple reports simultaneously

Paws Studio has been developed by the creators of the award winning Nipper Studio security auditing software. For a free evaluation of the software go to www.titania.com

Chinese Army unit is behind cyber espionage campaigns, researchers claim



Mandiant, the computer forensic and incidence response firm that got called in following the recent breaches of the New York Times' and Wall Street

Journal's networks, has issued a comprehensive report about a specific hacking group that they believe to be a unit of China's People's Liberation Army.

Dubbed APT1, this group is one of more than 20 APT groups with origins in China and has conducted cyber espionage campaigns against a "broad range of victims" since at least 2006.

In the last seven years, Mandiant's researchers have analyzed nearly 150 breaches that they believe were conducted by the group, but they point out that these attacks represents only a small fraction of the

total number of campaigns waged by APT1. They claim that the hacker group is "able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support," and that their analysis points to Unit 61398 of the People's Liberation Army (PLA's) being the APT1 group.

The building hosting the Unit is in same area from which APT1 activity appears to originate. "Either they are coming from inside Unit 61398, or the people who run the most-controlled, most-monitored Internet networks in the world are clueless about thousands of people generating attacks from this one neighborhood," Mandiant CEO Kevin Mandia commented the denial issued by China's Defence Ministry regarding the accuracy of the company's findings.

Mandiant estimates that the Unit is staffed by at least hundreds (and possibly even more) people that are trained in computer security and computer network operations and are proficient in the English language.

Successful ways of undermining cybercrime ecosystems



Most cybercrime is carried out by a loose confederation of independent contractors who work together when necessary through online forums and "partnerkas" that allow them to pool their resources, but these online criminal networks can be

foiled, according to a report by the Digital Citizens Alliance.

The report highlights recent examples in which others have weakened the glue that binds these criminal communities together by undermining trust relationships, isolating and apprehending key members, and making it more difficult for them to receive payment for their crimes. Tackling counterfeits, content

theft and intellectual property crime requires disrupting their channels of cooperation and payment. The easiest way to deter cyber criminals? Following the money and cutting off the payment source.

The key pillars that support most criminal commerce online include black market online bazaars, cybercrime joint ventures, and underground exchanges. Other report findings show that cyber criminals work through forums and "partnerkas" (when mutually beneficial), diversify their operations, and use pharmacy, malware, counterfeiting, and dating as popular schemes.

"The most uplifting part of this report are the examples of the digital community working with payment processors to stop and deter cybercrime," said Tom Galvin, executive director of Digital Citizens Alliance.

NetWrix has released its new User Activity Video Reporter



NetWrix has released its new User Activity Video Reporter tool that acts like a surveillance camera for critical servers and other IT systems by recording user activity for security, compliance, audit and troubleshooting.

By capturing metadata during the recording process for reporting and playback, the sophisticated VideoScape technology allows IT administrators to fast-forward or link directly to specific tasks or actions. This could include opening a window or starting a process, accessing or changing files, web browsing or

work done in management tools and applications.

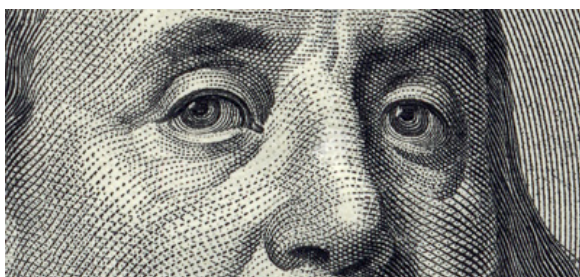
Complementing traditional configuration and change auditing solutions, NetWrix's new user activity monitoring software provides complete visibility of IT systems and applications that may not produce logs or enough information to investigate user behavior.

Many critical systems require administrator or vendor accounts to be given extensive permissions that could allow them to circumvent any change and configuration logging.

"Complete visibility over critical IT systems can be difficult, inefficient and expensive, but without 'who, what, when and where' audit detail, vital issues can go undetected and unresolved, risking security and compliance as well as compromising auditing requirements and troubleshooting," said Robert Bobel, Director of Product Management at NetWrix. "Our new User Activity Video Reporter captures every single user action for forensic review without having to filter through thousands of hours of activity or reports."

For more information visit www.netwrix.com

Investors demand more transparency about corporate cyber attacks



More than 70 percent of American investors are interested in reviewing public company cyber security practices and nearly 80 percent would not likely consider investing in a company with a history of cyber attacks, according to a new nationwide survey of investors released by HBGary. The survey of 405 U.S. investors also found that more than 66 percent of investors are likely to research whether a company has been fined or sanctioned for previous cyber security incidents.

“For some time, we have said that cybersecurity cannot be a 'checkbox' item on

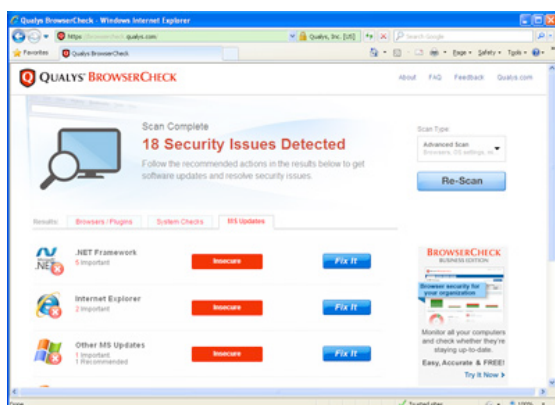
a company's operational to do list,” said Ken Silva, senior vice president of cyber strategy for ManTech's Mission Cyber & Intelligence Solutions Group. “This survey proves that today's investors are more educated about the damage cyber attacks can cause to a company's brand and financial bottom line. The high cost of cyber attacks cannot be understated.”

But, investors are not only looking at the actual attacks. Indeed, 66 percent of investors feel that corporate responses to cyber attacks are more noteworthy than the actual attack.

“This is good news,” said Jim Butterworth, chief security officer for HBGary. “Fortunately, corporations now have access to cutting-edge tools to conduct monitoring, incident validation, response and other key phases of incident response on their own – without need for expensive services.”

By a wide margin, the survey reveals investors are twice as concerned if a company had a breach of customer data (57 percent) versus theft of intellectual property (IP) (29 percent).

Qualys enhances its free cloud service BrowserCheck Business Edition



Qualys BrowserCheck Business Edition, the company's free cloud service, now gives organizations end-to-end automation for continuously monitoring which browsers, plugins, security settings and OS updates are present on users' computers.

IT administrators can now use the solution's web console to install BrowserCheck on employees' and contractors' computers, set up periodic automatic scans that are undetected by the users, and view reports of the results. Using the service, businesses can more effectively manage computer security across their organizations and show compliance auditors that systems are being kept up-to-date.

The enhanced Qualys BrowserCheck Business Edition web console automates the continuous monitoring of browser-related software on employees' computers and helps them update their systems when needed.

Philippe Courtot, chairman and CEO of Qualys, said: “By providing automated, continuous monitoring, Qualys BrowserCheck gives businesses a reliable way to measure and manage what they actually have so that they can follow best practices for security and address growing compliance mandates.”

Longline phishing attacks rely on mass customization



Proofpoint released a wide-ranging study that identified a new class of sophisticated and effective, large-scale phishing attack dubbed "longlining". Longlining, which is named after the industrial fishing practice of deploying miles-long fishing lines with thousands of individual hooks, combines successful spear phishing tactics with mass customization.

Using these techniques, attackers are now able to rapidly deploy thousands of unique, malware laden messages that are largely undetectable to traditional signature and reputation-based security systems.

Worse, despite their scale, these mass customized phish were effective enough to trick more than 10 percent of recipients into clicking on malicious content.

Unlike conventional mass phishing exploits, the "hooks" (email messages) used in

longlining are highly variable rather than identical, making them largely undetectable to traditional signature and reputation-based security gateways.

The messages are typically varied by IP address of origination, subject line and body content. The body content also includes multiple mutations of an embedded destination URL, which typically leads to a site with a positive reputation that's been successfully compromised prior to the attack. The compromised Web destinations are loaded with hidden malware either before, during or sometimes after the attack wave has begun.

Through the use of a distributed cloud of previously compromised machines and process automation to create high variance, attackers have been able to combine the stealth techniques and malicious payloads of spear phishing with massively parallel delivery. This means they can cost-effectively send 10,000 or even 100,000 individual spear phishing messages, all capable of bypassing traditional security.

Evernote breached, forces service-wide password reset



Evernote has notified its 50+ million users that the service's internal network has been breached by attackers and that they are forcing a password reset for all users.

"In our security investigation, we have found no evidence that any of the content you store in Evernote was accessed, changed or lost. We also have no evidence that any payment information for Evernote Premium or Evernote Business customers was accessed," Evernote CTO Dave Engberg wrote in a blog post.

"The investigation has shown, however, that the individual(s) responsible were able to gain access to Evernote user information, which includes usernames, email addresses

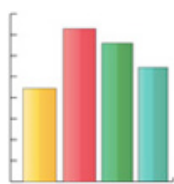
associated with Evernote accounts and encrypted passwords," he added.

Even though the passwords were hashed and salted - which algorithm is used to do this is not mentioned - the company has decided to make users reset their passwords just in case.

They are also required to enter the new password in other Evernote apps they use, and were notified of imminent updates to several of them.

"As recent events with other large services have demonstrated, this type of activity is becoming more common," wrote Engberg, possibly implying that the breach was effected via the exploitation of the Java 0-day vulnerability as was the case in the recent watering hole attacks that compromised Facebook, Apple, Twitter and Microsoft.

Google reports on non-court ordered FBI data requests



With every new Transparency Report that Google releases biannually since 2009, new information about data requests from government agencies are included. This last report, which spans July to December 2012, contains vague data about National Security Letters.

NSLs are a form of request for information that the FBI can make when they or other U.S. agencies are conducting national security investigations.

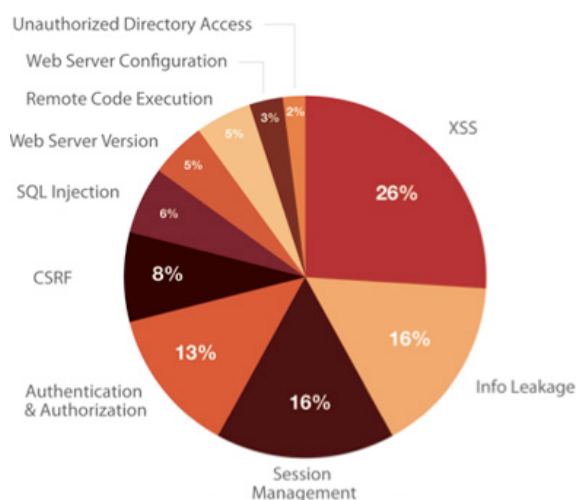
NSLs are an alternative to court ordered warrant and subpoena, and require only that the FBI director or another senior designee provides a written certification that proves that that the information requested is “relevant to an authorized investigation to protect against international terrorism or clandestine

intelligence activities.” Via NSLs, the FBI can request information such as the name, address, length of service, and local and long distance toll billing records of a subscriber, but cannot ask for things like Gmail content, search queries, YouTube videos or user IP addresses, as explained in Google's User Data Requests FAQ.

Also, the thing about NSLs is that their existence can be hidden from the investigated person. The FBI only has to write that the disclosure of the NSL may result in “a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person,” and Google (or any other provider) is forbidden to talk about the request.

In 2012 - and all years since 2009 except for 2010 - NSLs received by Google were between 0 and 999, and the users/accounts they applied to were between 1000 and 1999.

99 percent of web apps vulnerable to attack



A recent Cenzic report demonstrates that the overwhelming presence of web application vulnerabilities remains a constant problem, with an astounding 99 percent of applications tested revealing security risks, while additionally shedding light on pressing vulnerabilities within mobile application security.

The report reveals the massive number of vulnerabilities prevalent in web and mobile applications today.

It highlights the type, frequency and severity of vulnerabilities found and predicts which vulnerabilities will pose the greatest risk in web and mobile applications in production throughout 2013.

It also includes a study of mobile security threats, focusing on how data is transferred to and stored on mobile devices. According to Cenzic's findings, Input Validation (21 percent), Session Management (11 percent) and Privacy Violation (25 percent) combine to account for 57 percent of mobile vulnerabilities.

These results suggest that while storing unencrypted sensitive data on sometimes-lost mobile devices is a significant cause for concern, the often-unsecured web services commonly associated with mobile applications can pose an even bigger risk.



Becoming a malware analyst by Zeljka Zorz

There are few jobs in this industry that seem as appealing and interesting to me as that of a malware analyst. In my mind, these professionals were waking up each day to continue a complex game not unlike the Glass Bead Game from the eponymous novel by Herman Hesse - a pure pursuit of the mind that makes connections where there are seemingly none, all for the sake of solving intricate puzzles in order to satisfy their curiosity and cravings for intellectual challenges. But I was wrong!

To satisfy my own personal craving to know what it was all about, I decided to contact a number of malware analysts working for some of the most high-profile security companies out there and ask them a few questions.

The traits and skills of good malware analysts

Some malware researchers, like McAfee Lab's Principal Research Architect Igor Muttik, entered the field in the '80s, when the anti-virus programs were only appearing and there was no multi-billion AV industry yet. Others, like Jana Barborikova, a Junior Virus Analyst at Avast, have been in it for less than a year.

But the one thing they all have in common - beside insatiable curiosity - is the satisfaction of knowing that they are keeping users safe. In fact, the willingness to help people is one of the main qualities of a good malware researcher according to Muttik. "In this regard what we do is very similar to the work of the doctors, police and firefighters," he muses.

"What are the others?" I asked. A high IQ, he says. "Anyone can be a good programmer but to be successful in computer security one has to be smarter than the best of the attackers. This requires dedication and the more brain cells you can contribute - the better!"

"Crucial for malware analysts is the ability to get a full overview of what modern malware does, how it does it and why it's doing it," Bogdan Botezatu, Senior E-Threat Analyst with Bitdefender, tells me.

"Patience is also mandatory. Decrypting a piece of malware with server-side polymorphism or tracking down its behavior in a virtualized environment can get extremely frustrating. Last but not least is a strong sense of ethics. The lack of affiliation with black-hat or cybercriminal groups is just a start. Since we're trusted with lots of confidential information and access to zero-day samples or still unpatched exploit code, we need to know that no employee would use the code for malicious purposes."

He sees the job more as a vocation. "I know quite a few antivirus researchers who are designated economists, MDs or, as in my case, historians or journalists, but are experts on cybercrime. Of course, IT-related educational backgrounds make it easier to learn how computers, operating systems, network communication and applications work, but it is not mandatory."

Kaspersky Lab Senior Malware Analyst Denis Maslennikov agrees. "The most important thing is to be interested in this field, because if you are, this interest will drive you and guide you while you search for new knowledge and experience. It's more about the knowledge you have than about the diploma. If you have

some basic background and are able to learn new stuff you can become malware analyst."

He also reiterates Botezatu's opinion on ethics. "Stay out of the black / grey area. No antivirus company will hire you or trust you with zero-day code if you have worked for or have been affiliated with exploit writers, black hat hackers or unauthorized pen-testers. Most disclosure about ongoing operations follows a strict vouching process in which the candidate receives approval or denial from peers in the industry."

The ability of not letting failure to put you off is another crucial trait according to Barborikova. "An analyst cannot be afraid to try new approaches and think outside of the box."

AN ANALYST CANNOT BE AFRAID TO TRY NEW APPROACHES AND THINK OUTSIDE OF THE BOX

Finally, you need to be ready and able to communicate. "The best reverse engineer in the world is useless if she cannot report her findings in a clear and concise way," points out Guillaume Lovet, Senior Manager FortiGuard's Labs in EMEA at Fortinet.

But what kind of base knowledge is a must-have? Or, at least, is highly recommended?

"Most malware nowadays requires analysts to understand assembly languages. Learning and understanding this will unlock many doors in the field of malware analysis," says Liam O'Murchu, Manager of Operations, Symantec Security Response.

Barborikova concurs, and that is why she's currently focusing on learning them. "The analyst does nothing without some programming skills, fundamentals of networking and a basic knowledge of operating systems," she adds.

"Reverse engineering – although the focus of antivirus research – is not everything a candidate needs to understand. Most of the time, you will need to build your own tools and extend them to suit your new purposes," Botezatu weighs in.

"If you already understand assembly language, you should start learning a programming language (such as C++ and Python), as you're going to use it to automate day-to-day tasks, write custom scripts to help you with your work or develop state-of-the-art disinfection routines that will reach millions of customers on the next update."

Lovet agrees, and considers some developer skills in scripting languages almost mandatory. He also points out that - unlike him - not all analysts have been professional C++ developers before becoming analysts, and that he finds this a significant advantage when it comes down to reverse-engineering malware pieces, which are usually coded in C++.

What none of them (or the companies they work for) consider important is having certifications.

"We do not require any certifications for new malware engineers joining our team. The most important thing is to have hands on experience analyzing malware or performing security investigations," says O'Murchu.

How does one become a malware researcher?

The roads that lead to this are many and various. Maslennikov and O'Murchu studied, respectively, information security and computer engineering at college. For the former, the road was very straight - while still at university, he got a call from Kaspersky Lab and was offered a malware analyst position.

The latter went through several jobs such as a security tester for an internet kiosk company and working at an anti-spam company that was ultimately bought by Symantec. "We were given a tour of the new Symantec offices and as soon as I entered the malware analysis lab I knew that was the job I wanted. I was fortunate to have the opportunity to transfer into that department and short time later and have been here since," he says.

Muttik and Barborikova have an education in natural and formal sciences. Both were interested in a career in information security, and Muttik practiced reverse-engineering viruses as a hobby.

A previously mentioned, Botezatu studied history and journalism, but was also interested in reverse-engineering malware since he was a teenager. Following a stint as a network administrator for his university, he applied for a job at Bitdefender two times. After having overslept and missed the interview the first time, he worked half a year as a tech journalist before trying his luck again. This time, he was recruited by the company's communication team.

"Since joining Bitdefender, I've worked in a multitude of fields, from technical communication to anti-malware research and new product development. I grew to understand security from tracking down malicious activity to actually developing solutions to mitigate it, and speaking about developments in the industry at international conferences. As part of a cross-disciplinary team, we're exposed to everything that happens in the anti-malware field, so we have a full perspective on the industry," he shared.

Lovet became a malware analyst after a 2-year-long developer experience. "Being a de-

veloper satisfied my analytic and synthetic mind, as well as my creativity, yet it lacked the 'passion' component," he says, adding that he began working as a Malware Analyst at Fortinet in 2004.

"At the beginning, we'd manually process loads of legacy DOS viruses - because we needed to have detection for those to earn some certifications. These were fun times: studying 20+ viruses per day is the equivalent of playing poker online, at 5 different tables at once: you play a LOT of hands, and gain experience faster," he shares.

After becoming the AV Team leader, he turned more toward researcher and presenting at international conferences such as AVAR, EL-CAR, and Virus Bulletin.

"Eventually, I got promoted to AV and IPS team manager, then senior manager. Today, I still do my share of research (last year I presented 2 papers at BlackHat in Amsterdam), and some management of people. This was my choice, in order to diversify my skills. It is perfectly possible to stick to purely technical tasks and progress in the company aside of the management ladder, up to the rank of Fellow, which equates a VP rank in the management career," he points out.

Malware researchers' typical working day and the tools they use

"During my work I deal mainly with web malware," shares Barborikova. "I go through a list of potentially dangerous URLs and select domains which are actually malicious. Then I analyze samples, especially HTML and PHP files. Apart from handy internal tools developed in our virus lab department I use free-ware tools like VirtualBox, Process Monitor or Wireshark and online deobfuscators and decoders."

"We use IDA Pro and OllyDbg for reverse engineering. And our own tools for intelligence and monitoring (probes and honeypots), says Lovet. "On the secluded replication machines, where we safely run viruses to study their behavior, we don't use virtual machines, as some malware spots those. On the mobile malware side, we have our own in-lab, secluded GSM network.

We built a base-station with a modified USRP board. The software part is OpenBTS, an open source system. When we register infected phones to that network, we can therefore trace what they do on the network: send SMS, place calls, etc."

IDA and OllyDbg are O'Murchu's "weapons of choice," as well, since they are standards for the two primary tools any malware analyst needs: a disassembler and a debugger.

"We have separate machines that we use for malware analysis. In addition to having all the tools needed for analysis installed, these machines are also isolated with no Internet connection. This prevents any malware from escaping when we are testing it," he says.

"We generally run the threat to look at observable behaviors first, then dig deeper as needed. Using hex editors and file format parsers and learning about different file formats is also a big part of a malware analyst's role. For example if a PDF file is being used to distribute a piece of malware, then analyst will need to become familiar with how PDF files are created and how to break them apart."

Botezatu says that he is not sure where his typical day ends and where it starts. "Antivirus research is a 24-hour mission - if your phone rings or the SMS alert beeps in the middle of

the night, you take off to work, or at least VPN into the company immediately," he notes.

"If an outbreak has been detected, we start developing a removal tool for computer users who are not running a Bitdefender solution.

If everything is running normally, we proceed to solving support tickets, clustering new malware and improving heuristics, while keeping an eye on security (highly private) mailing lists for new samples and developments. You know - the save-the-world-while-having-coffee activities."

"As far as tools are concerned, we're using a lot of readily available tools such as Far Manager, IDA, Process Explorer, Process Monitor, Malzilla, and Wireshark. But the heavy lifting is done with proprietary tools built in-house, tools that don't even have names. In the fight against malware, it's every man for himself, we're mostly using tools that we develop ad-hoc, ranging from unpackers to utilities for clustering files, rebooting remote machines or controlling operations off-site," he concludes.

Maslennikov says that there is really no typical working day, as there is always something new and / or urgent going on. He does his testing on two desktops with Windows and Linux and a lot of smartphones with different OS, and can't do without the Far file manager, IDA, Hiew and a number of various internal tools. Oh, and coffee - plenty of it, and often.

A SMALL NUMBER OF THREATS PUSH THE BOUNDARIES OF WHAT IS POSSIBLE

Finally, I asked them:

What surprised them the most during their current career?

"I have been in the security industry for almost 10 years, and I am continuously surprised by the new attacks the malware cyber criminals dream up," says O'Murchu. "Although the vast majority of attacks are predictable and nothing out of the ordinary, there is always a small number of threats that push the boundaries of what is possible."

The threat that has amazed him the most was Stuxnet. "We had never seen a piece of malware capable of changing how physical machinery works. That was a threat that really pushed the boundaries of what malware can do," he added.

Botezatu has been most surprised by the success of the Slammer worm, the virality of Conficker, the way cyber-crooks made easy money with the Rogue AV campaigns and the complexity of the TDSS family.

"But the piece of malware that went through our hands and surprised the entire world was Flamer, a piece so elegantly designed that it tricked the user into acting as a mule for the stolen data," he shares. "It took espionage to a whole new level: the ability to prioritize importance of stolen data, the way it carried the data to a gateway and the fact that it lacked compression and obfuscation, hiding its code in plain sight. This was clearly not the result of a single man, but rather the work of a team of specialists."

And while Barborikova, who has only been doing this for a year, says that she naturally often encounter things that are new for her, Lovet says that the thing that fascinates him the most is that cybercriminals have not begun exploiting mobile phones earlier.

"Back in 2006, I predicted that they would, since a smartphone was basically a computer with something more: an integrated payment system (i.e. premium numbers). It'd simplify a

lot the business model you need to set up to turn infected machines into cash," he pointed out.

Nevertheless, it didn't really happen before 2011, and even now, he says, the scale on which it's happening is still moderate as compared to the PC world.

Conclusion

I am very grateful for the peek that these experts gave me into their profession, and I hope that you have enjoyed this as well, especially if you're contemplating a (new) career in malware research.

Common sense says that cyber attack will never stop, but just become different, so put in you "pros" column the fact that you'll rarely be bored at your job and that, if you become good at it, will probably never experience a lack of job offers.

Zeljka Zorz is the Managing Editor of (IN)SECURE Magazine and Help Net Security.



**DAILY OR WEEKLY
SECURITY NEWS
RIGHT IN YOUR INBOX**

net-security.org/infosecuritynews.php



Review: Nipper Studio

by Berislav Kucan

Developed by UK-based Titania Ltd., Nipper Studio is an interesting solution that takes a whole new approach towards security auditing. Wouldn't it be great to be able to analyze the security of vital aspects of your network in just a couple of seconds? It may sound overly optimistic, but Nipper Studio aims to do just that.

A network is comprised of different devices, from switches and routers to firewalls and other security appliances. A number of problems can arise: they can be misconfigured, left unpatched or get maliciously modified.

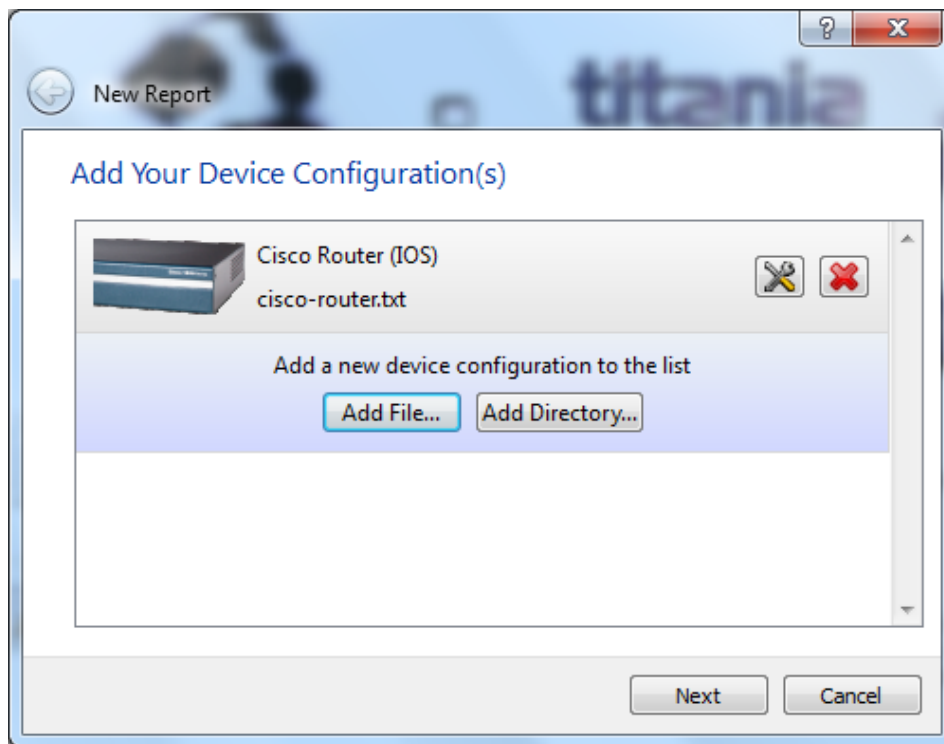
Auditing these devices can take a toll on your budget, especially if you are using outside contractors for the job. Titania saw a market in this and their Nipper Studio aims to be a more cost effective, flexible, and better-fitting solution for this problem.

With a large number of plugins built in-house, Nipper Studio is powered by an intelligence engine that is fed with the the configuration file of a selected device. It then analyzes it and in a record time delivers a clear picture of potential problems.

The product itself is a standalone application that can run on a number of different systems - Windows, Mac OS X, as well as the most popular Linux distributions (CentOS, Fedora, OpenSUSE and Ubuntu). The installation is very straight forward. You need to visit the vendor's homepage, choose the download file (depending on the OS, it varies from 7 to 69 MB) and grab your serial number/activation code combo.

I counted over 100 different devices that Nipper Studio can analyze and the list includes all the major appliances. For an actual list of currently supported devices, please go to www.titania-security.com/nipperstudio/devices

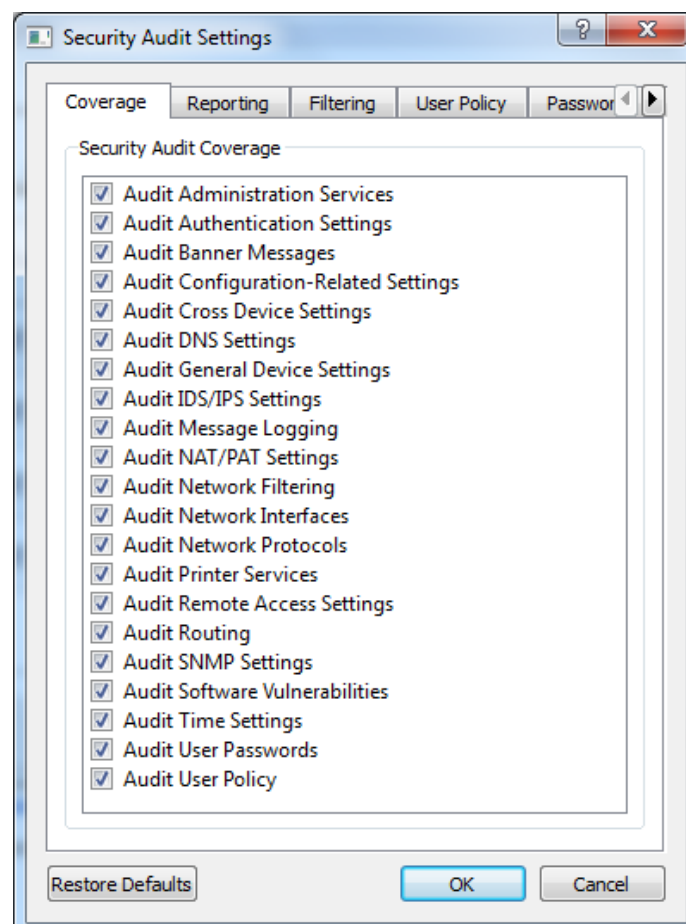
The administrator just needs to download the configuration file from one or more devices that need to be tested and open it in Nipper Studio.



Starting the analysis process by adding the configuration file.

The analysis setup procedure is packed with configuration options and the level of detail customization is impressive. In the security audit coverage screen, you can select the

scope of the audit by (de)selecting specifics such as NAT, IDS/IPS settings, authentication details, network interfaces, etc.

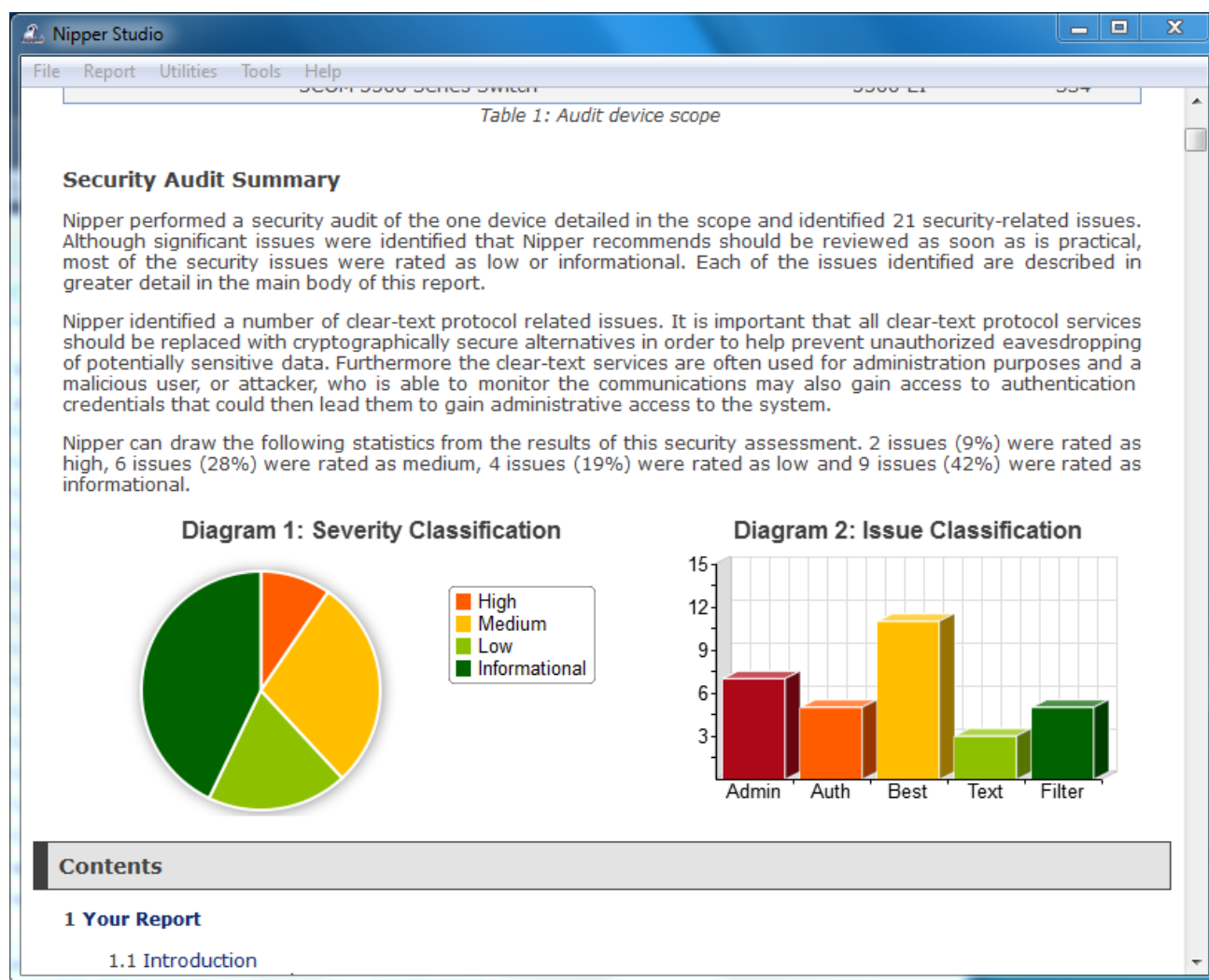


Setting up the security audit scope.

The app lets you be as creative as possible when setting up different filters. There is even a section where you can decide whether to use Nipper Studio's own rating system or CVSS v2 to optimize the analysis toward your actual target environment. When the setup is over, you just click the "Finish" button and within a couple of seconds, the report appears.

The quality of the report is top notch! Every alert or issue found is followed with a large

chunk of information that helps you understand the problem and its potentially impact, and a set of recommendations to mitigate the issue. If you do any modifications on the device, you can just reboot it, get the latest configuration file and re-asses it with Nipper. In this case (XML exports needed) you can use the compare functionality to analyze the security status of the same device based on different scan time frames.



Security audit summary that opens up the report.

Besides XML, the reports can be exported into a number of different formats including HTML, PDF, CSV, and SQL. Needless to say, you can custom edit any of these export types to suite your needs. In the reporting module, I also liked the possibility of excluding some portions from the report or even adding your personal comments to any found issues. Any

report can be customized with your company logo and details.

Nipper Studio is an extremely handy application that solves the problem of network auditing in a simple and cost-effective way, and should easily find its way into every security professional's arsenal.

Other potential uses may be completely unexpected and cause harm. These uses will not be welcome. To help them make informed decisions, people need to be able to understand how information will be used and informed about what choices they have about its use.

Social networking is now a normal part of life, with most users still unaware of the privacy and security implications of the personal data they make available online. What type of problems do you expect careless users will have in the future? Are we moving towards a society where there is no privacy at all?

Social networking has certainly become, and will remain, an integral part of many people's daily lives. Considering the amount of information we share and store online with these interactions, one might think the general notion of privacy is dead.

However, privacy remains tremendously relevant, especially in the social-media-infused, data-rich world in which we live.

Consumers expect strong protections, as they are increasingly aware of the amount of information available about them online and how companies can secure information about them.

According to results of a recent Microsoft-commissioned survey of 1,000 U.S. adults, 45 percent feel they have little or no control over the personal information companies gather about them while they are browsing the Web or using online services.

Our current generation is growing up on social networks and is constantly interacting with their mobile devices. Yet even as they share more information, they also want to maintain control over how much they share, who they share it with and how it is used. They don't want their data to be later used or shared in ways they didn't expect or that don't provide value to them.

More and more people want to share information, but they also want the organizations that hold their information to use it responsibly and to protect it.

More and more people want to share information, but they also want the organizations that hold their information to use it responsibly and to protect it.

The over-sharing phenomenon fueled by Facebook users drives cybercriminals to innovate. Now we have automated social engineering which enables attackers to easily mass profile a lot of people.

Should the companies running social networking sites make sure their users understand the privacy implications of their actions even though it hurts their bottom line?

People have increasingly become the victims of social engineering attacks as criminals are progressively seeking to install spyware or other malicious software to trick them into handing over passwords or other sensitive financial or personal information. These online criminals find it much easier to exploit human

nature rather than exploit software vulnerabilities.

In addition to criminals using online information in an attempt to gain access to your accounts, there can be other implications resulting from information shared online.

In a recent Microsoft study about online reputation management, 14 percent of respondents believe they have been negatively impacted by the online activities of others, even unintentionally so. Of those, 21 percent believed it led to being fired from a job, 16 percent being refused health care, 16 percent being turned down for a job, and 15 percent being turned down for a mortgage.

To best protect themselves against these on-line threats, people should be armed with more than just the latest technology solutions.

Since awareness and education are the first defense in avoiding online risks, Microsoft has made free advice easily accessible at the Microsoft Safety & Security Center, where we have easy-to-follow guidance and resources, including several video tutorials, for protecting one's privacy.

Do we need more government regulation in order to protect consumers from increasingly privacy-invading organizations?

Government regulation, industry self-regulation and innovation around privacy from organizations all have an important role to play in advancing privacy. Industry self-

regulation can play key a function by offering flexible means for protecting privacy across contexts.

In addition, Microsoft has long supported baseline federal privacy legislation to create a common underlying framework for companies. Recommendations from regulators can motivate a lot of investment in privacy protection and innovation within organizations, and it can also help advance self-regulatory frameworks.

We're optimistic that 2013 will be the year that a self-regulatory approach to online privacy succeeds. Otherwise, the alternative is a piecemeal of regulations enacted by governments around the globe and less protection than consumers deserve and privacy advocates desire.

Government regulation, industry self-regulation and innovation around privacy from organizations all have an important role to play in advancing privacy.

What privacy-related initiatives does Microsoft participate in? How do you teach users to be more responsible with their sensitive information?

We know our customers want and expect strong privacy protections to be built into our products, devices and services, and for companies to be responsible stewards of consumers' data. We've been focused on this area for more than 10 years as part of Trustworthy Computing at Microsoft.

But, that's just the start. People also need more information about their privacy options and help controlling their personal information online. As part of our longstanding commitment to privacy, we're kicking off a new video

series called Privacy in Action. These videos, which are available at www.microsoft.com/yourprivacy, illustrate many of the privacy options in Windows 8, Windows Phone 8 and Microsoft's Personal Data Dashboard (where customers can make choices about how Microsoft uses their data).

I'm proud of the dedicated group of privacy professionals here at Microsoft that works diligently every day to help protect your privacy as we deliver new innovations.

Resources like www.microsoft.com/privacy are just the latest examples of how we take our privacy responsibilities seriously and put people first.

Application security testing for AJAX and JSON

by Dan Kuykendall



Application security professionals and application developers may not be aware of it, but their web application scanners are leaving big vulnerabilities wide open.

New programming interfaces and formats associated with rich, new custom and mobile applications are difficult for traditional scanners to crawl. Cyber-criminals are already taking advantage and using vulnerabilities to access back-end servers where critical information resides.

Don't be lulled into a false sense of security by traditional scanners, programming, security and testing methodologies. A detailed review of new application architectures and data formats can help you identify and remediate vulnerabilities before applications are rolled out.

In this article we will examine AJAX and JSON—how your web application scanner addresses these formats today, and what you can do to augment its efforts.

AJAX—amazing strides in web applications, but major headaches for web scanners

Traditional web application scanners were designed to crawl static HTML pages. Many modern applications and web services have very little static HTML to crawl, rendering scanners unable to assess them. New technologies like AJAX aren't neatly tucked behind HTML pages, yet we know vulnerabilities exist in these layers.

In AJAX applications, HTML is used to setup the framework that harnesses the power of XML HTTP Request (XHR) objects, which make calls to specific interfaces. AJAX is a collection of technologies and an approach to web development that has been the major force behind making web apps incredibly rich

and user friendly. Technically, AJAX stands for Asynchronous JavaScript and XML, and the key term here is “asynchronous.” Older web applications maintained a synchronous relationship between each new page and the response to the user. Now the asynchronous capabilities of AJAX mean that a single web page can function as an entire application, à la Google Maps or Gmail.

With AJAX applications, the user can stay on a given page as the page requests new data from the server and presents it to the user. Usually, there is a designated area on the page for presenting data, and the user’s actions or events initiate a series of steps that the page performs on the user’s behalf.

Gmail is a classic example of AJAX, where the inbox is the designated area for presenting data. As you click on specific messages, the page requests new data to display the content of the email. A closer examination of an AJAX-based web mail application reveals the following steps:

1. When the user clicks on the email subject in the list, a JavaScript function called “funcShowEmailContent” will execute the following steps:
 - a. Set up an event handler called “funcDisplayEmailContent.”
 - b. Perform an XmlHttpRequest with the email message ID.
 - c. End
2. Once the function ends, the browser is not forced to wait for the response. It is free to allow other activity to take place (asynchronously), such as deleting another message or choosing to read a different email.
3. Eventually the response arrives, and the browser passes it to the event handler “funcDisplayEmailContent,” which processes the response and populates the designated area with the email content the user has requested.

Google Maps provides another great example of AJAX in action. When you want to go north on the map, you click up and the next map grid instantly appears (by performing these AJAX routines in the background). AJAX makes the application even more user-friendly

by preemptively caching the next map grid in the browser, causing it to show up almost instantaneously. With such great strides in application functionality and usability come major headaches for web application security scanners. Some of the primary reasons web scanners struggle with AJAX include:

Deep links - Many web scanners can handle the first instance of an AJAX page, and some can even handle the second instance. Think of the first instance as the inbox page on Gmail and the second instance as actually clicking into an email message. But it becomes progressively harder for scanners to delve into the third layer and beyond. An example of the third level would be adding user contacts in Gmail.

Referencing attackable locations - It is easy to reference the page and parameter of an attack location in a traditional, HTML-based web application. But AJAX complicates this action because user requests/responses all happen on a single page with many possible user events. Going back to the web mail application example, a vulnerability may reside where a user is replying to an email, but this first requires the user to click on an email subject line and then to click the “reply” button. The combination of URL and user events can be highly complex and difficult for a scanner to reproduce.

JavaScript Object Notation (JSON) - JSON is an alternative to XML for sending data back and forth. An entirely different format, JSON is increasingly used by AJAX sites and programmers because it uses fewer characters to send the same amount of data. However, if a web scanner can’t parse JSON, it can’t test that page.

Document Object Model (DOM) - The DOM is sufficiently complex to deserve its own article. With the DOM, the web page is not sent to the browser as HTML. Instead, the web server creates a data structure (called the DOM) within the browser and the browser interprets that data structure to create the page. Since web scanners were designed to interpret HTML, the DOM creates obvious obstacles to crawling and attacking some web applications.

How can you ensure better security coverage for AJAX?

Determining whether your web scanner can crawl AJAX applications is not easy. With traditional web applications, web scanners typically provide a list of the links they have crawled, enabling you to check for a particular link in question.

This process breaks down with AJAX, because it enables multiple iterations of content on a given page. The web scanner may be able to discover a page, but miss the second and third iterations. And the request / response traffic sent back and forth to create the second and third iterations of the page may only appear in scanning reports as fragments of pages. The data in those requests may appear in complex formats as well. Only the most experienced AJAX developers will understand what the scanner results show.

As a result, extra steps to check for good scanning coverage of an AJAX application may be required, such as:

- Enabling the web application scanner's detailed logging feature (if available).
- Setting up the scanner to run through a proxy like Paros, Burp or WebScarab, and saving the logs for manual examination.
- Once the logs are collected, they will appear as a garbled mess of HTML and data requests back and forth to the server. The easiest way to see if a page has been scanned is to find some unique content and search for it.
- The next step is to see if the web scanner actually attacked the server requests. The best way to do this is to train your scanner by inputting a unique value into a form field. Next, search for the value and see if the web scanner is attacking it with alternate requests.

AJAX demands some creativity on the part of application security testers, but it's well worth the effort to protect vital back end servers from compromise.

JSON and Mobile JSON—make sure your scanner has you covered

JSON is an alternative to XML for sending data back and forth between applications (in-

cluding web applications) and servers. JSON is increasingly used in AJAX applications, including Google Web Toolkit and mobile applications. Some programmers prefer it to XML because JSON uses fewer characters to send the same amount of data.

The primary problem JSON poses for typical web application scanners is that it's simply a newer format. Web scanners must be able to decipher JSON and insert attacks to test the security of the web application interfaces. If they are not familiar with JSON, they will not provide coverage. JSON is very easy to read, evidenced by this example:

```
{
  "firstName": "John",
  "lastName": "Doe"
}
```

Use your scanner to find out if your web application is using JSON. Turn on the detailed logging with request/response traffic feature to review the logs for instances of JSON traffic and any attacks. If the scanner does not provide detailed logging, simply set up a proxy (e.g. Burp or Paros) and run the scan through it.

Start with a limited scan of just a page that uses JSON, and once you capture the traffic in the proxy, you can check to see if the scanner requests include the JSON traffic and attacks.

Many mobile applications use JSON as well. Mobile apps send data back and forth to servers just like web applications, and are vulnerable to many of the traditional web app exploits.

Some web application scanners make a clear distinction about their inability to scan mobile applications. However, some vendors are blurring the lines regarding mobile application scanning ability based on the ability to import proxy logs.

Make sure you know the extent of your scanner's capabilities, and determine a strategy and process for testing mobile application security manually if need be.

The real issue is whether web scanners can understand the traffic being sent back and forth between mobile applications, and create attacks to test for security flaws. The scanner's ability to interpret and attack JSON traffic (the preferred data transfer mechanism for mobile apps) will be a primary determinant. Most web scanners are not as familiar with the JSON and REST formats used by mobile applications, so even if they are fed recorded traffic they have no ability to create attack variations.

Stay tuned for the next installment providing more details about new application programming formats such as AMF and REST, and more details about security testing for mobile applications.

While web application scanners remain a vital part of the security testing model, professionals must become familiar with the underlying technologies of rich custom and mobile apps, and the extent of their existing scanners' testing ability.

Dan Kuykendall is Co-CEO and CTO of NT OBJECTives (www.ntobjectives.com) and can be contacted at dk@ntobjectives.com

FEATURED SOFTWARE: NetWrix Change Reporter Suite



NetWrix Change Reporter Suite automates and simplifies the auditing of critical IT systems across the entire IT infrastructure. With one simple deployment you can efficiently audit critical IT systems such as: Active Directory, Exchange, VMware, EMC Celerra/VNX, NetApp Filer, SCVMM, Windows Server, Network Devices, SQL Server, SharePoint and many more - while staying within a reasonable budget.

NetWrix Change Reporter Suite generates reports that include complete information on every single change that has occurred in the IT infrastructure and can be used for detailed forensic analysis. Unlike traditional log management solutions, NetWrix makes it very easy to find relevant answers to key questions: who changed what, when and where, including "before" and "after" values for modified settings. The product streamlines compliance to HIPAA, SOX, PCI, GLBA, FISMA and many other regulations, provides an easy-to-use solution that drastically improves IT infrastructure visibility and internal security.

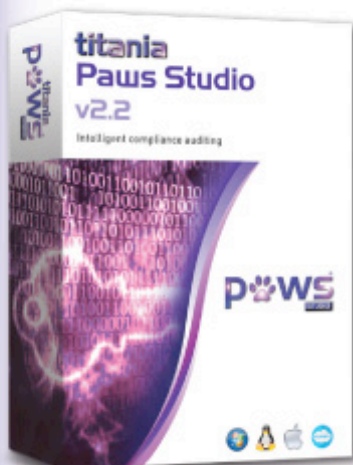
For more information visit: www.netwrix.com/trial

Need help with compliance?



Use Paws Studio to audit your workstations and servers

Paws Studio is efficient, easy to use and cost effective. The software provides comprehensive reporting and management summaries to appeal to all levels of your organization.



...from the creators of award winning Nipper Studio software

With Paws Studio you can:

1. Produce remote compliance audits using remote connectivity or audit offline with our unique Data Collector
2. Use the Remedy Table to quickly solve potential compliance issues
3. Create and modify your own policies using the Paws definition editor

evaluate for free at
www.titania.com

Compliance Checklist	Paws Studio
Antivirus	✓
Spyware	✓
Audit Policy	✓
Files & Directories	✓
Windows Firewalls	✓
Password Policies	✓
Password Warnings	✓
Permissions	✓
Registry Settings	✓
Software Updates	✓
Installed Software	✓
Illegal Software	✓
Software Versions	✓
User Policies	✓
User Rights	✓

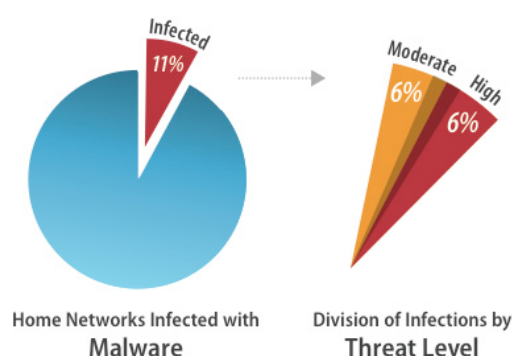


enquiries@titania.com
T: +44 (0) 1905 888785



Malware world

Mobile network infections increase by 67%



Kindsight released a new report that reveals security threats to home and mobile networks, including a small decline in home network infections and an increase in mobile network infections. Highlights include:

- The rate of home network infections decreased from 13 to 11 percent in Q4; 6 percent exhibited high-level threats, such as bots, rootkits and banking Trojans.

- The ZeroAccess botnet continued to be the most common malware threat, infecting 0.8 percent of broadband users.
- In mobile networks, 0.5 percent of devices exhibited high threat level malware, which increased by 67 percent from 0.3 in Q3.
- The number of Android malware samples was 5.5 times larger in Q4 than in Q3.

This report also marks the first time that Kindsight has released annual metrics from its security research.

Findings from 2012 include:

- 13 percent of home networks in North America were infected with malware in 2012 with 7 percent of broadband customers, infected with high-level threats.
- Botnets were responsible for four of the top five high-level threats on home networks in 2012, including ZeroAccess, TDSS, Alureon and Flashback.
- Almost 50 percent of infected home networks had a botnet issue in 2012.

Malware authors revert to phishing approach to trick bank defenses



Banking malware that performs Man-in-The-Browser tricks such as injecting legitimate banking sites with additional forms, hijacking the authenticated session to add a new payee and transfer money in the background and so on has had success in the past.

But, as financial institutions have reacted to their existence and have implemented systems for monitoring the online sessions between customers and their web applications, the actions of malware such as Tinba, Tilon, Shylock and others employing the MitB approach get increasingly detected and thwarted. Consequently, the malware authors have had to resort to new tricks to avoid detection.

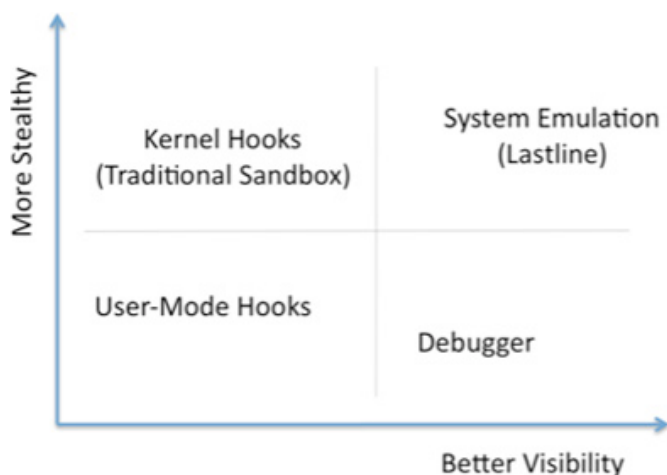
Trusteer has discovered that Tinba and Tilon have been recently modified to try out a simpler approach: phishing and blocking users from the actual banking page.

"When the customer accesses the bank's website, the malware presents a completely fake web page that looks like the bank login page. Once the customer enters their login credentials into the fake page the malware presents an error message claiming that the online banking service is currently unavailable. In the meantime, the malware sends the stolen login credentials to the fraudster who then uses a completely different machine to log into the bank as the customer and executes fraudulent transactions," explains Trusteer CTO Amit Klein.

"If the login or transaction requires two-factor authentication (OTP tokens, card and reader, etc.) the malware captures this information as part of the fake login page. Using this tactic the malware never lets the customer reach the bank's login page, which prevents backend security systems from being able to detect malware anomalies in the session and identify the fraud."

The good news is that fraud attempts associated with these new versions of Tinba and Tilon are still limited. The bad news is that banks who haven't covered both attack vectors - session hijacking and credentials theft - are putting their customers at risk.

The security threat of evasive malware



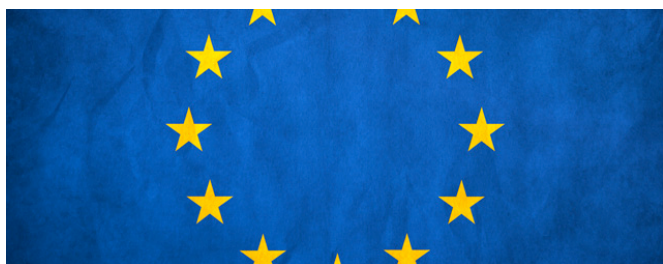
Lastline has released a new report that looks at how malware authors are able to exploit the limited visibility of automated malware analysis systems (sandboxes) and ensure that

targeted attacks and zero day exploits remain successful. The use of stalling codes is resulting in a growing trend of evasive threats.

The report highlights two techniques currently used by malware authors: environmental checks and stalling code. While environmental checks have been well documented, stalling code is the latest technique being utilized to spread malware. It delays the execution of a malicious code inside a sandbox and instead performs a computation that appears legitimate.

Once the sandbox has timed out, the evasive malware is free to execute. The report finds that stalling codes are particularly troublesome because they "can no longer be handled by traditional sandboxes (even if the trick is known)."

Old school malware used for spying on European govts



Kaspersky Lab's team of experts published a new research report that analyzed a series of security incidents involving the use of the recently discovered PDF exploit in Adobe Reader (CVE-2013-6040) and a new, highly customized malicious program known as MiniDuke - a backdoor was used to attack multiple government entities and institutions mostly in Europe.

"MiniDuke's highly customized backdoor was written in Assembler and is very small in size, being only 20kb," said Eugene Kaspersky, Founder and CEO of Kaspersky Lab.

"The combination of experienced old school malware writers using newly discovered exploits and clever social engineering to compromise high profile targets is extremely dangerous," he added.

The MiniDuke attackers are still active at this time and have created malware as recently as February 20, 2013. To compromise victims, the attackers used extremely effective social engineering techniques, which involved sending malicious PDF documents to their targets.

The PDFs were highly relevant, and were rigged with exploits attacking Adobe Reader versions 9, 10, and 11, bypassing its sandbox.

Once the system is exploited, a very small downloader is dropped onto the victim's disc that's only 20kb in size. This downloader is unique per system and contains a customized backdoor written in Assembler. When loaded at system boot, the downloader uses a set of mathematical calculations to determine the computer's unique fingerprint, and in turn

uses this data to uniquely encrypt its communications later.

It is also programmed to avoid analysis by a hardcoded set of tools in certain environments like VMware. If it finds any of these indicators it will run idle in the environment instead of moving to another stage and exposing more of its functionality by decrypting itself further; this indicates the malware writers know exactly what antivirus and IT security professionals are doing in order to analyze and identify malware.

If the target's system meets the pre-defined requirements, the malware will use Twitter (unbeknownst to the user) and start looking for specific tweets from pre-made accounts. These accounts were created by MiniDuke's Command and Control (C2) operators, and the tweets maintain specific tags labeling encrypted URLs for the backdoors.

These URLs provide access to the C2s, which then provide potential commands and encrypted transfers of additional backdoors onto the system via GIF files.

Based on the analysis, it appears that MiniDuke's creators provide a dynamic backup system that also can fly under the radar. If Twitter isn't working or the accounts are down the malware can use Google Search to find the encrypted strings to the next C2.

This model is flexible and enables the operators to constantly change how their backdoors retrieve further commands or malcode as needed.

Bitdefender researchers have later discovered a version of MiniDuke that has been operating for at least 21 months, and Kaspersky experts have recently discovered two of its previously unknown web-based infection mechanisms.



11 arrested in takedown of prolific ransomware gang



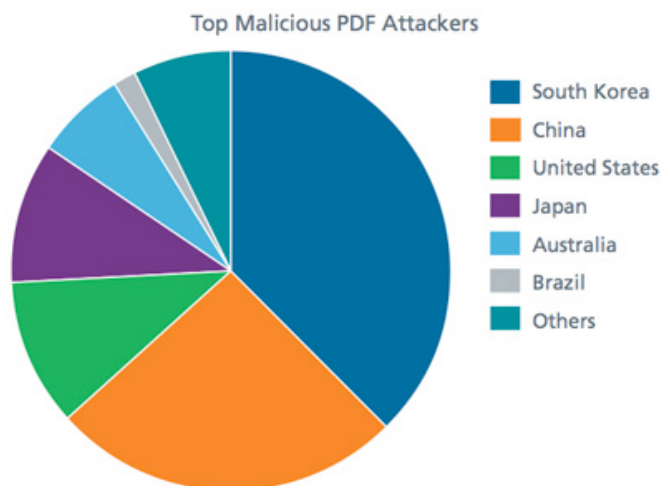
The Spanish Police, working closely with the European Cybercrime Centre (EC3) at Europol, have dismantled the largest and most complex cybercrime network dedicated to spreading police ransomware (Reveton). It is estimated that the criminals affected tens of thousands of computers worldwide, bringing in profits in excess of one million euros per year.

Operation Ransom resulted in 11 arrests. Six premises were searched in the province of

Málaga, where IT equipment used for the criminal activities was confiscated. In addition, investigators seized credit cards used to cash out the money that victims paid via Ukash, Paysafecard and MoneyPak vouchers, as well as around 200 credit cards which were used to withdraw €26 000 in cash prior to the arrests.

The financial cell of the network specialized in laundering the proceeds of their crimes, obtained in the form of electronic money. For this, the gang employed both virtual systems for money laundering and other traditional systems using various online gaming portals, electronic payment gateways or virtual coins. They also used compromised credit cards to extract cash from the accounts of ransomware victims via ATMs in Spain. As a final step, daily international money transfers through currency exchanges and call centers ensured the funds arrived at their final destination in Russia.

Malicious URLs eclipsing botnets as malware distribution leader



McAfee Labs revealed that sophisticated attacks originally targeting the financial services industry are now increasingly directed at other critical sectors of the economy, while an emerging set of new tactics and technologies are being implemented to evade industry-standard security measures.

“We are seeing attacks shifting into a variety of new areas, from factories, to corporations,

to government agencies, to the infrastructure that connects them together,” said Vincent Weafer, senior vice president of McAfee Labs.

In Q4 2012, McAfee Labs identified the following trends:

- Cybercriminals realized that user authentication credentials constitute some of the most valuable intellectual property stored on most computers.
- The decline in the number of infected systems controlled by botnet operators is driven in part by law enforcement efforts to bring botnets down
- Increase in infections beneath the OS - The volume of Master Boot Record-related malware climbed 27 percent to reach an all-time quarterly high.
- Malicious signed binaries circumvent system security - The number of electronically-signed malware samples doubled over the course of Q4.
- Mobile malware continues to increase and evolve - Cybercriminals are now dedicating the majority of their efforts to attacking the mobile Android platform, with an 85 percent jump of new Android-based malware samples in Q4 alone.

Penetrating and achieving persistence in highly secured networks

by Bogdan Botezatu



Only a couple of years ago, cyber-criminals almost exclusively targeted Internet-connected end-users and companies. Now, high profile attacks target isolated, highly secure corporate or business environments. This paper describes the challenges of breaching such systems, achieving persistence for as long as possible, and payload delivery mechanisms.

Ever since government and companies adopted the Internet on a massive scale, cyber-criminals have become interested in breaching these critical infrastructures and monetizing them in various ways, with particular focus on disruption and information theft.

The continuous siege from outside hostile parties has prompted businesses, enterprises, governments and mission-critical service companies such as utility providers to isolate their networks and render them inaccessible (or limit their accessibility) to the outside world. As a rule, the more critical the network is, the higher the degree of isolation.

How is successful penetration carried in isolated environments?

One of the most frequent mistakes when deploying a highly secure network is allowing it to be extended without the intervention of a network administrator. Many times, employees trade security for usability without even realizing they are exposing the network to outside threats. Wireless access points installed without notification and without proper security, public and private network bridging through proxy servers or the installation of other devices for tethering (i.e. mobile phones or 3G modems) can and will annihilate any safety mechanism the network administrator has in place.

An advanced persistent threat attack begins with either exploiting one of the technical vulnerabilities exposed above, or by social engineering the user into breaking security protocols of the organization, such as the restriction

to plug in a USB drive in computers that are part of the private network.

The goal of an advanced persistent threat is to gain prolonged access to an organization's resources for monitoring and/or sabotage.

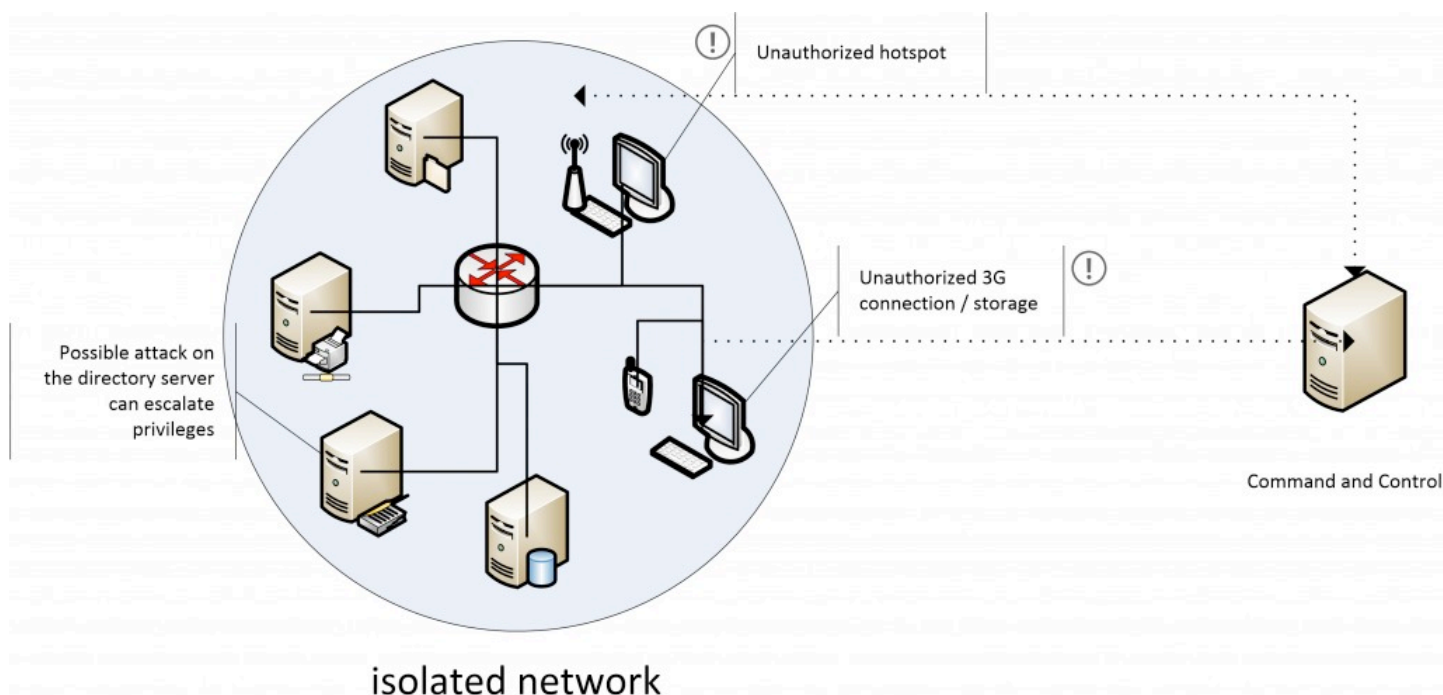


Figure 1: Vulnerable spots of a protected network. Wireless extensions and unauthorized gateways to the Internet expose the network to outside attackers.

Exploitation of an unauthorized extension of the network with wireless devices is the easiest method for a cyber-criminal in close proximity to gain access to a protected environment. In the absence of a strong audit of the network configuration, legitimate users could add a wireless router in a spare Ethernet outlet or even bridge a wireless connection to work in access point mode.

Most of the time, these are not deliberate acts of sabotage, but fatal mistakes aimed at enhancing usability of a restrictive networking environment (i.e. sharing the local internet connection with a smartphone or creating a wireless connection in the meeting room without consent from the network administrator).

This way, any nearby attacker can probe the Wi-Fi space for unprotected or poorly-secured networks, then use open-source tools to attack WEP, WPA, LEAP or even VPNs and other proprietary wireless technologies. Once the network has been identified, cracking the

rudimentary encryption allows the attacker to connect to the network to access resources.

Mitigation:

- As a system administrator, you should always disable any Ethernet outlet that is not in permanent use directly from the patch panel in the server room.
- Configure your DHCP server to lease IPs by MAC addresses only.
- Talk to employees about the importance of keeping the network isolated at all times. Make them understand that any modification to the network infrastructure will have disastrous effects.
- Use Wi-Fi space monitoring tools to detect wireless signals originating from your facility. A simple \$10 key fob Wi-Fi signal detector is often enough to identify illegal access points in your organization.

Unregulated access to the Internet via 3G modems or 3G tethering defeats the purpose of isolating the network environment. Whenever the user connects to the internet through a personal device from a machine that is part of the isolated network, they become perfect targets for blended threats – malware delivered via well formatted e-mail messages that trick the user into either downloading an infected and apparently innocuous attachment (such as a PDF or document file) or prompt the user to visit a legitimate website hosting malware.

Mitigation:

- Enforce security policies on all computers connected to the network. Disable or render USB ports physically inaccessible to prevent storage devices from being connected to the PC. This way, users can't inadvertently plant malware and can't move stolen information outside of the network.
- Block Bluetooth and wireless on host computers to disallow file transfers and interconnection with user-owned devices.

Personal storage and multimedia devices arbitrarily plugged into network computers can act as highly effective vectors not only for malware, but also for the information that escapes the network to the attacker's command and control server. This approach, although less effective than directly sending data to the attacker via the Internet, has proven much more successful in high-profile attacks such as the Flamer incident.

Last, but not least, **mind the physical security of the facility**. Even the most secured networking environment is useless if physical access to the facility, data center or server room is lax or unregulated. Skilled social engineers can cut their way through office buildings; determined attackers can convince or coerce personnel with access to the building (employees, janitorial team, maintenance crew) to plant devices for them and open security breaches at the network perimeter. The Darpa-funded Pwnie Express products for instance are disguised as power strips and can be connected to the network, then used by attackers for persistent access to the network over 3G.

Achieving persistence in isolated environments

For long-term exploitation of the isolated network, attackers use a combination of malware tools that take care of deployment, data and password gathering, scanning the network perimeter and reporting. These tools keep a low profile and are specially designed to evade antivirus detection. The evasion is possible because, most of the time, the cyber-criminal team behind the attack uses brand-new code that has never been seen in the wild by antivirus vendors.

Zero-day exploitation against client software plays a key role in the stealthy dissemination of the payload across the network, aided by unconventional malware programming using less known APIs and next to no obfuscation of the malicious code.

A key advantage of an isolated environment is that it is considered clean and virus-free. By design, they allow no intrusion from the outside, as they are rarely connected to other networks.

More than that, one of the most effective means of defense against malware is only partially functional: in the absence of a permanent connection to the internet to deliver hourly malware signature updates, the antivirus uses only outdated signatures and behavioral patterns – two technologies that are highly ineffective against brand-new malicious code engineered to conceal suspicious behavior.

We know advanced malicious code used in breaching isolated networks often comes unencrypted, unpacked and needs no internet connection to operate. These features are critical in evading antivirus detection that monitors code changes, entropy and typical malicious behavior. This was the case of Flamer, the world's largest piece of malware, which avoided detection by having the exact opposite features of modern, commercial malware. In the absence of an antivirus solution to flag the intrusion, it is up to the network administrator to mitigate a possible infection by constantly monitoring network traffic and ensuring that security policies are enforced.

Blended threats: original source of infection

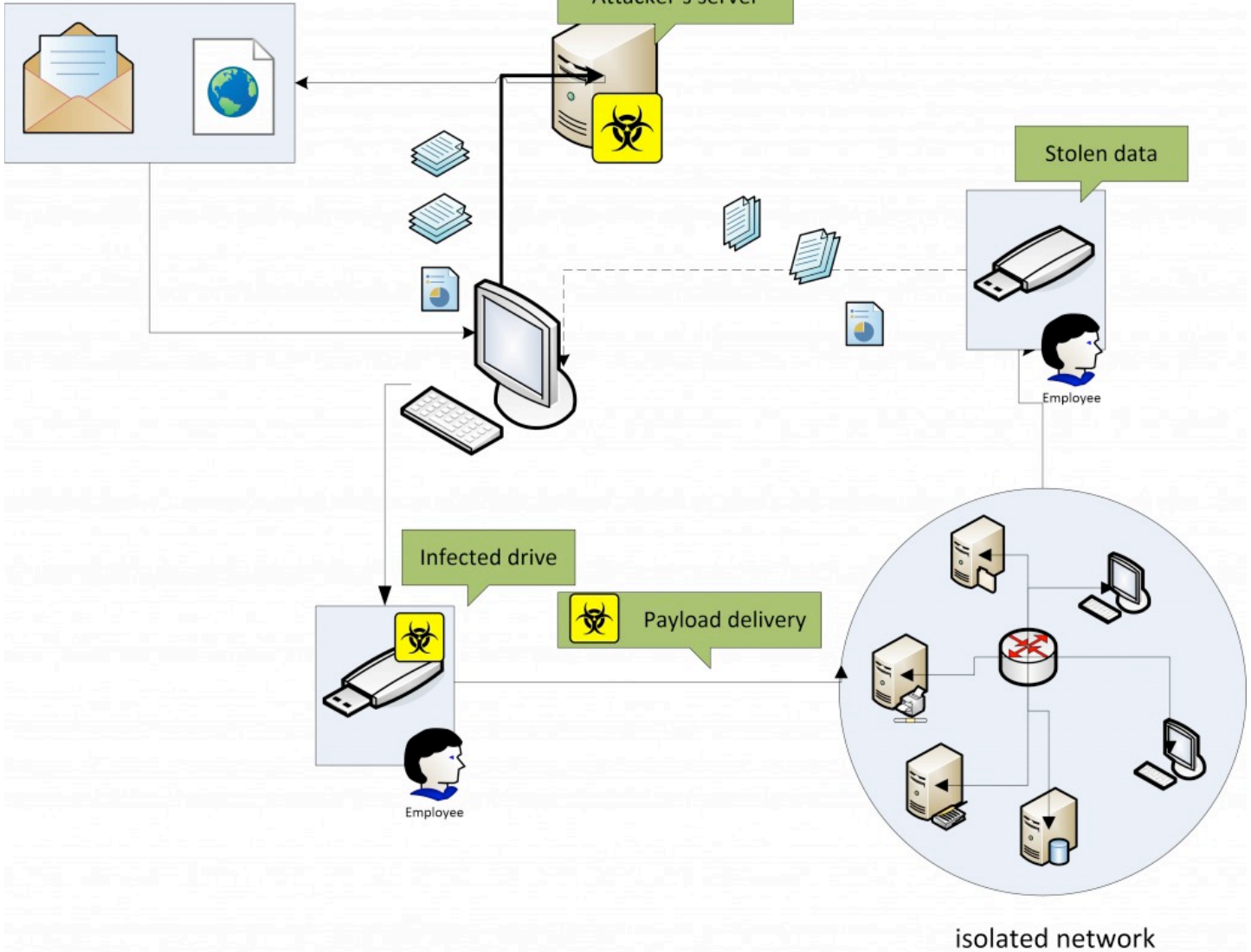


Figure 2: The circuit of a Flamer-infected device: the employee is used both as a vector of infection and as a carrier for stolen data.

Payload delivery and operation mechanism

One of the most frequently-encountered misconceptions is that a piece of malware is only harmful when it can actively communicate with the command and control server.

While this is mostly true for consumer-grade malware that specializes in sending spam, harvesting addresses or manipulating banking transactions, the outlook is different for military-grade e-threats of the size and complexity of Stuxnet, Duqu or Flamer.

Malware specializing in cyber-espionage rarely relies on the local connection to the Internet to siphon data outside of the perimeter. That approach would likely trigger firewall alerts; the huge amount of data sent to the

C&C server is also likely to be visible to packet inspection applications such as Wireshark, and that will compromise the operation. More likely, the attackers use an employee's removable device as transportation between the isolated network and an unmonitored, compromised workstation at the employee's home, for instance.

Not all malware is tailored for espionage and persistence, but is rather focused on delivering a payload or fulfilling a mission.

This was the case of Stuxnet, the world's first piece of malware that was tailored to subvert an industrial system to compromise the production process at the Natanz-based uranium enrichment facility in Iran.

The e-threat was particularly designed to seize control the Siemens Simatic WinCC SCADA applications controlling centrifuge machines and did not affect computers or networks that did not meet specific architecture requirements.

Conclusion

Isolated networks are the ultimate fortresses, but they are penetrable. The ecosystem is as safe as its weakest link: the human user, be it employee, system or network administrator.

The Stuxnet and Flamer incidents have demonstrated that even the most secured networks are no match for cyber-weapons, instruments designed to go where no piece of malware has gone before. These instruments, which likely share the same origin, prove that highly-skilled cyber-criminal groups can always take the game one step further and create more and more sophisticated threats to outsmart defense mechanisms.

Bogdan Botezatu is the Senior E-Threat Analyst at Bitdefender (www.bitdefender.com). When he is not documenting sophisticated strains of malware or writing removal tools, he teaches extreme sports such as surfing the web without protection or rodeo with wild Trojan horses. He believes that most things in life can be beat with strong heuristics and that antimalware research is like working for a secret agency: you need to stay focused at all times, but you get all the glory when you catch the bad guys.

Want to reach a large audience of security pros by writing for (IN)SECURE?



Send your idea to editor@insecuremag.com



RSA Conference concluded its 22nd annual event in early March at the Moscone Center in San Francisco. A record number of over 24,000 attendees attended approximately 394 sessions, keynotes, peer-to-peer sessions, track sessions, tutorials and seminars, which featured 620 speakers.

More than 360 companies across the cybersecurity landscape showcased the tools and technologies that will protect personal and professional assets now and in the future.

RSA Conference 2013 highlights include:

- This year's Innovation Sandbox program featuring interactive white boarding sessions, the opportunity to speak with industry-leading experts and the top 10 finalists' presentations to a panel of judges.
- Remotium was named Most Innovative Company at RSA Conference 2013 by the Innovation Sandbox's judges' panel, which was comprised of technology, venture and security industry thought leaders.
- Moderated by Scott Hartz, CEO, Taasera, Inc., "Ten Years Later - The National Mission to Secure Cyberspace," featured a 10-year anniversary discussion around the Depart-

ment of Homeland Security and the National Strategy to Secure Cyberspace. Former DHS Secretary Tom Ridge and former Cybersecurity Czar Howard Schmidt looked back at the growing sophistication of cyber attacks over the last decade and how industry and government have worked together.

- For the first time, RSA Conference introduced a CISO Viewpoint track where CISOs and CIOs participated in a variety of sessions that highlighted how business and security are intersecting. CISOs and speakers from companies like eBay, Google, Bank of America, Visa, Zappos and Johnson & Johnson spoke on a variety of issues including big data, risk management, and the psychographics of CISOs.
- Security Mashup Debate sessions pitted industry professionals against each other in topics like pen testing tools and security awareness training.



Philippe Courtot, Qualys CEO and Mikko Hypponen, Chief Research Officer at F-Secure.

“For 22 years, leading minds in cybersecurity have gathered with us from around the world to address the security threats of today and tomorrow,” said Sandra Toms LaPedis, Area Vice President and General Manager of RSA Conference.

“The Conference once again served as forum for professionals to examine the evolution of the information security industry and how it is affecting businesses, countries and individuals. We look forward to growing with the industry and helping organizations protect themselves in the face of today’s cyber landscape.”



Not all of the companies showcasing their offerings on the expo floor have come prepared to release new solutions, but among those who have, here are the ones whose announcements and presentations garnered the most attention:

SpiderOak: Crypton

Crypton is an application framework for building cryptographically secure cloud applications, which offer meaningful privacy assurance to end users because the servers running the application cannot read the data created and stored by the application.



In the past, using cloud technologies meant definitively sacrificing privacy (having plaintext information viewable by 3rd party servers). Crypton allows companies and developers to realize "zero-knowledge" privacy cloud environments out-of-the-box. This is accomplished by transparently handling the complicated cryptography layers through Crypton and allowing companies to focus on domain specific challenges instead of figuring out how to push privacy and security after-the-fact.

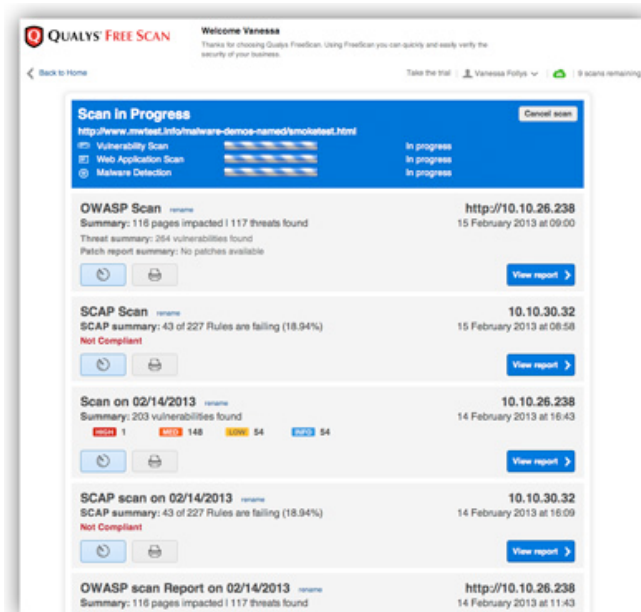
Qualys: FreeScan service

Qualys has expanded its popular FreeScan service, which is used by organizations all over the world to quickly test online whether their computers, networks, web sites, and web applications are at risk from the latest threats.

Qualys FreeScan now integrates a variety of security and compliance scans into a single, uniform console.

Patch Tuesday PC Audit. This scans PCs to find missing updates and patches from business software, such as Microsoft Windows, Oracle Java and Adobe Flash and Reader. It identifies which patches are required to address vulnerabilities that are found and pro-

vides links for downloading the necessary updates. After fixes have been installed, this scan can be run again to verify that computers are up-to-date.



OWASP Web Application Audit. This tests web applications, either inside a company's network or on the Internet, to see if they comply with the latest OWASP industry-standard guidelines for defending against online attacks such as SQL injection and cross-site scripting (XSS).

It organizes any issues that are found according to the corresponding OWASP categories and helps application developers fix application weaknesses.

SCAP Compliance Audit. This tests computers within a company's network to see if they comply with leading security configuration benchmarks, such as the U.S. Government Configuration Baseline (USGCB), which is required by many U.S. federal agencies and organizations that do business with the government.

Web Site Scan for Vulnerabilities and Malware. This performs a comprehensive check of a company's web site for server and application vulnerabilities, hidden malware and SSL security configuration errors.

Additionally, FreeScan now supports the deployment of virtual scanners for scanning internal systems and web applications.

Spyrus: Secure Pocket Drive Build Your Own Linux Program

The Secure Pocket Drive (SPD) Build Your Own Linux Program with Spyrus' Secure Pocket Drive bootable USB product line includes a set of Linux Builder Utilities, which gives users the ability to create and manage their own personal, portable, and secure Linux operating environment.



The software includes a security initialization utility that generates new cryptographic keys in the SPD hardware, sets password and login policies, and locks/unlocks the encrypted compartment as needed for updating the operating system or applications.

In addition, "admin utilities" are provided to reset the user password by the administrator and to change the administrator password when required. Finally, Microsoft Windows and Linux compatible utilities are provisioned directly on the boot compartment of the SPD to allow the user to manage their password.

Secure Pocket Drive with your favorite version of Red Hat, Ubuntu, SLAX, or SE Linux is bootable on almost any Wintel or Apple Macintosh desktop or laptop. This makes it ideal for individual home users and supports enterprise BYOD initiatives.

SPD can be set up in two different configurations: Read-Only and Read-Writable. Both configurations can be used online when connected to a network or the internet or offline with no network, and both employ the same Suite B On Board hardware security infrastructure that is built into the Spyrus Hydra Privacy Card family.

All Secure Pocket Drives use only digitally signed memories by Spyrus. Moreover, hardware-based XTS-AES 256-bit full disk encryption (NIST SP800-38E) encrypts and secures the operating system, applications,

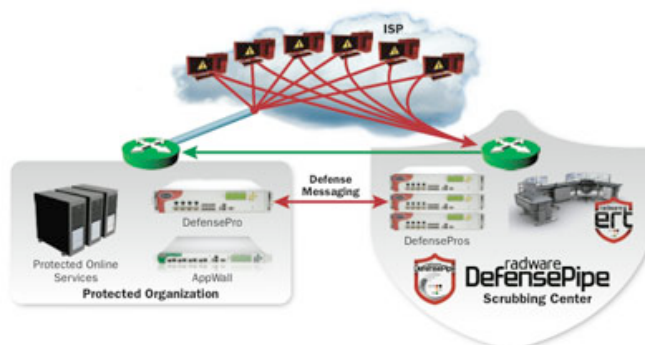
and data on the drive. SPD also has built-in security checks that make it extremely difficult, if not impossible, to break into the drive without rendering it inoperable to the hacker.

Radware: DefensePipe

DefensePipe is an integrated solution for mitigating DDoS attacks that threaten to saturate a customer's Internet pipe, or the "outside line" that connects enterprises to the web.

DefensePipe is a solution for end to end attack mitigation on-premise and in the cloud that automatically engages once the customer's Attack Mitigation System detects that pipe saturation is imminent.

The organization's suspicious Internet traffic is immediately diverted to the DefensePipe cloud based scrubbing center where it is distanced further from the protected network and its scalable resources can mitigate high volume attacks.



Once the traffic is "cleaned" it is then sent to the organization and regular operations continue once the attack has ceased.

The integration of on-premise AMS and DefensePipe provides wide coverage of attacks, including SSL based attacks, application layer attacks, low and slow, network floods, known vulnerabilities and egress traffic attacks. The mitigation is automatically initiated - there is no need to wait for human intervention or to divert the traffic to a remote data center in order to start it.

Also included is access to Radware's Emergency Response Team (ERT), a "round the clock" staff of security experts who mitigate the attack with the customer during the entire attack campaign.

Pwnie Express: Pwn Pad

Pwn Pad is a tablet loaded with wired and wireless pentesting tools.

The sleek form factor makes it an ideal product choice when on the road or conducting a company or agency walk-through.



Core features:

- Android OS 4.2 and Ubuntu 12.04
- Large 7" screen, powerful battery
- OSS-Based Pentester Toolkit
- Long Range Wireless Packet Injection.

HW accessories:

- TP-Link TL-WN722N (atheros usb wifi)
- Sena UD100 (Bluetooth USB)
- USB Ethernet
- OTG cable (USB host mode).

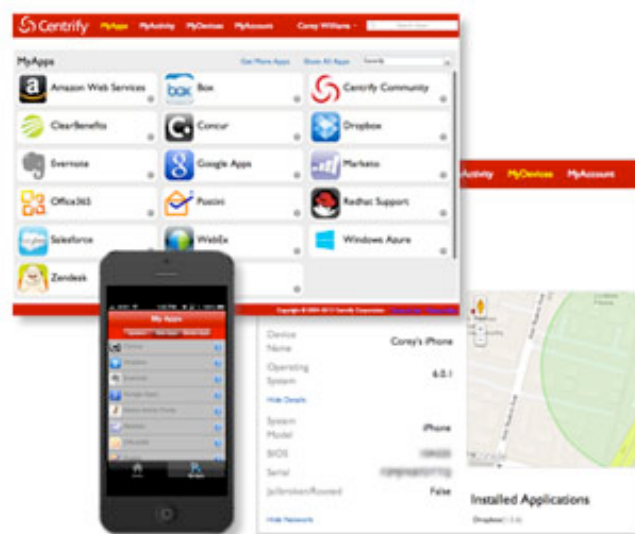
The toolkit includes:

- Wireless tools (Aircrack-ng, Kismet, Wifite-2, Reaver, MDK3, EAPeak, Asleap-2.2, FreeRADIUS-WPE, Hostapd)
- Bluetooth tools (bluez-utils, btscanner, blue-log, Ubertooth tools, Web Tools, Nikto, Wa3f)
- Network tools (NET-SNMP, Nmap, Netcat, Cryptcat, Hping3, Macchanger, Tcpdump, Tshark, Ngrep, Dsniff, Ettercap-ng 7.5.3, SSLstrip v9, Hamster and Ferret, Metasploit 4, SET, Easy-Creds v3.7.3, John (JTR), Hydra, Medusa 2.1.1, Pyrit, Scapy)

Centrify: Centrify for Mobile 2013 and Centrify for SaaS 2013

Centrify for Mobile 2013 and Centrify for SaaS 2013 is a set of integrated capabilities enabled by the Centrify Cloud Services platform that delivers secure, enterprise-class mobility with integrated application Single Sign-on (SSO).

A unified approach to managing an employee's digital identity that spans on-premise, cloud and mobile resources provides the visibility and control required for IT organizations to achieve compliance, reduce costs and mitigate risks, while also increasing productivity and securing access for their mobile workforce. The Centrify Cloud Services platform integrates application Single Sign-on, Mobile Device Management, Mobile Application Management, mobile authentication and Mobile Container Management services in a single solution that enables organizations to easily manage mobile and cloud initiatives via an infrastructure they already own — Active Directory.



Centrify for SaaS supports hundreds of cloud-based apps, including Salesforce.com, WebEx, Box.net, and hundreds more. In addition, the service offers the MyCentrify portal where users obtain one-click access to all their SaaS apps from their PC, and can utilize self-service features that let them locate, lock or wipe their mobile devices, and also reset their Active Directory passwords or manage their Active Directory attributes. A mobile app version is also available on the Apple App Store and Google Play.

Booz Allen Hamilton: Cyber4Sight Threat Intelligence Services

Cyber4Sight Threat Intelligence Services uses multiple data sources to identify and monitor an organization's unique cyber security profile, determine its "attack surface," and deploy military grade predictive intelligence to anticipate, prioritize and mitigate cyber threats.



Cyber4Sight combines the science of Big Data with the art of analysis and information gathering to give clients a holistic, forward-looking cyber security program. This service is the result of a significant multi-year investment Booz Allen has made to create an infrastructure that globally integrates data collection, aggregation and analysis and engages cyber analysts from a myriad of disciplines.

The Services center on:

- All-source data: Booz Allen's data collection, aggregation and analysis platform filters millions of pieces of data from thousands of sources in real-time
- Intelligence analysis: Company analysts provide 24/7/365 threat monitoring to produce actionable and predictive information. Managed client services: The suite of Cyber4Sight products includes: trip-wire reports, situation reports (SITREPs), spot reports (SPOTREP), daily summaries and requests for analysis and response.

Allegro: Allegro Cryptography Engine (ACE) Embedded FIPS Cryptography Toolkit

Allegro added FIPS 140-2 compliant Allegro Cryptography Engine (ACE) to the RomPager suite of embedded internet toolkits.

Early networked desktop PCs and servers were unprepared to address the new security implications of network connectivity. The same is true for many of today's embedded systems which presents a significant new security concern that must be addressed immediately and systematically. ACE is a platform independent, high performance, resource sensitive, FIPS cryptography engine specifically engineered for the rigors of embedded computing.


The module provides embedded systems developers with a common software interface to enable bulk encryption and decryption, message digests, digital signature creation and validation, and key generation and exchange.

ACE includes a platform independent, government-certified implementation of the NSA Suite B defined suite of cryptographic algorithms, and makes embedding standards-based security protocols into resource sensitive embedded systems such as military, energy and healthcare embedded applications fast, easy and reliable.

Fortinet: FortiGuard cloud-based sandboxing and IP reputation services

The FortiGuard cloud-based sandboxing service uses behavioral attributes to detect malware by executing them within a virtual environment. This serves as an additional protection layer that complements the FortiGate's existing antivirus engine and its inline lightweight sandbox.

Suspicious files can be submitted automatically to the new hosted service for further scanning without significantly impacting a FortiGate's performance. In addition, FortiCloud has added a new feature that serves as the online sandboxing portal, which provides detailed status and visibility into the scanned results. FortiGuard Labs continually investigates and monitors IP's that are compromised or behaving abnormally. The FortiGuard IP Reputation Service uses a number of different techniques, including historical analysis, honeypots and botnet analysis to provide immediate protection against wide scale automated attacks. The service also continuously learns from a global footprint of threat sensors, tracking malicious events to IP addresses in real time.



Social engineering: An underestimated danger

by Dr. Amy Burrell

I've been involved in a lot of discussions about information security over the past few years and it never ceases to amaze me how much emphasis is put on the technical aspects of IT security at the expense of considering how human failures can lead to data breaches.

In particular, there is always a lot of concern about how we protect IT systems against sophisticated attacks by super intelligent hackers whilst completely neglecting the risks posed by staff not adhering to policies and procedures or their vulnerability to being socially engineered to give away information.

The poor implementation of data protection rules, e.g. inadequate checks and balances in place, can pose a major threat to information security. Vulnerabilities may also emerge where people are lazy, or do not understand the potential consequences of failing to meet policy standards.

However, there are also lots of ways people might be manipulated through social engineering into giving away information that would facilitate an attack, and this risk is often overlooked. In this article I will outline what social

engineering is and how it poses a risk to information security. If I also manage to provide you with ideas for mitigating the risk from social engineering, all the better.

What is social engineering?

Social engineering is the act of manipulating people into performing actions that compromise security or divulging confidential information. As reformed computer criminal Kevin Mitnick points out, it is much easier to trick someone into giving you a password than make the effort to crack into the system.

Tricks of the trade - how do they do it?

Perhaps the most well known means of social engineering is phishing – the act of creating a legitimate looking email or letter from an institution or a person in a position of authority

with the aim of gaining access to personal or confidential information. I would be surprised to come across anyone who has not received an email from a Nigerian Prince or someone similar offering them the opportunity to make some quick cash by holding onto some money for them. All they need is your name, address, and bank details...

Whilst such phishing attacks are clumsy and easy to spot, the sheer volume of emails sent, combined with the fact we all still receive them, suggests that the senders are achieving some level of success. Furthermore, some groups of people are singled out by social engineers as they are seen as more susceptible to phishing scams. Take for example the pyramid schemes that commonly target elderly people who are perceived to have the money to invest and time on their hands, and may be lonely and starving for attention. Another example is the recent money laundering scam targeting students, unemployed people, and foreign nationals.

The desperation to earn money in the poor economic climate, and/or poor knowledge of UK legislation and banking norms, help the social engineer to persuade targets to sign up as “money transfer agents” or “payment processing agents” (see www.bbc.co.uk/news/business-21578985). The targets then effectively launder the criminals’ money through their own bank account and take a percentage as “payment” for their services. This is, of course, illegal and can have dire consequences for the victims who may end up with a criminal record and/or being denied banking services.

There is evidence that phishing attempts are becoming more sophisticated. I myself recently received a very legitimate looking email purporting to be from a very well-known high street bank, and the only reason why I wasn’t fooled is that I am not actually a customer of that particular bank.

There are also examples of named individuals working in large firms being specifically targeted with official looking emails issuing them with a subpoena and informing them they need to appear in court (in the USA). These emails, of course, had malicious links embedded within them.

The targeted nature of such attacks has given rise to the term “spear phishing” and I would not be surprised to see such attacks continue to evolve in the future as their targeted nature increases the chances of people complying with requests made in the email.

Although phishing is perhaps the most well-known social engineering tactic, it is by no means the only one. There are numerous other ways a social engineer can persuade people to part with confidential information or permit them to access places they shouldn’t be allowed to. For example:

- **Familiarity exploit** - This is one of the best tactics and is a cornerstone of social engineering. In a nutshell, you are trying to make it appear perfectly normal to everyone that you should be there. For example, pretend to be an employee to gain access – identity cards can be stolen or mimicked and uniforms can be purchased (have a quick search on eBay if you don’t believe me!). Combined with poor access control procedures, this makes for easy pickings for the social engineer.

- **Pretexting** – the social engineer will create and use an invented scenario (i.e. the pretext) to engage the target in a way that increases their chances of divulging information or acting in a different way. This is also known as blagging.

- **Diversion theft** – the social engineer persuades the persons responsible for a legitimate delivery that the consignment is requested elsewhere and steals the contents.

- **Baiting** – the real-world Trojan horse. This relies on the curiosity and greed of the victim by offering “too-good-to-be-true” investment opportunities.

- **Impersonating someone in a position of authority** – this is a common tactic used by social engineers. In emails, they will claim to be a peer/prince, a law enforcement agent, or anyone else that could be perceived as an authority figure. In person, an air of confidence and the ability to lie convincingly can gain a social engineer access to all sorts of places.

- **Tailgating** – it is surprisingly easy to tailgate people into secure premises. The polite practice of holding doors open is a social engineer's dream. To be honest, most people hate confrontation and are unlikely to challenge you anyway.

- **Hostility** – contrary to what you might think, the social engineer may wish to, on occasion, draw attention to themselves by being very hostile. This is because people just want to get rid of angry people and they are much more likely to obey your wishes when you are angry, so it works well when asking people to

open doors for you or provide information on the location of things. A good real-world example of this is to start an argument with someone as you approach a checkpoint (e.g. if you are trying to sneak alcohol into a festival) and security staff may be more likely to wave you through instead of searching you.

- **Quid pro quo** – this is where a social engineer will offer something for something else in return. For example, disgruntled employees may be approached to provide information in exchange for cash.

CONTRARY TO WHAT YOU MIGHT THINK, THE SOCIAL ENGINEER MAY WISH TO, ON OCCASION, DRAW ATTENTION TO THEMSELVES BY BEING HOSTILE

There are lots of techniques and approaches that the social engineer can access to facilitate their work. For example:

- **Surveillance** – identifying the targets' routine helps determine the best way to approach them. However, the approach does not always need to be direct. Take for example a scenario where a group of employees regularly go to the same pub on a Friday night. Conversations after a few alcohol beverages can lead to sharing of confidential information.

- **Maximizing on naivety** – I once sat on a commuter train at peak time when the woman in the seat behind me decided to pay a bill over the phone. By the time she got through to payment services I could have had a pen and notepad ready and would have been able to write down all of her credit card information (including the 3 digit security code on the back of the card!). Imagine what I could have done with that information.

- **Using social networks** – LinkedIn, Facebook, Twitter and other social networks contain a mountain of information. It is surprising how much personal data you can access about someone from their social media profiles. Knowing this kind of information could allow strangers to strike up a conversation with you under the pretense that they know you. Once your barriers are down, they can

start asking more confidential questions to gain the key information that they want. Some people also post where they are at a given time and even information on when they are going on holiday! Imagine that you are a social engineer and you know Bob is going on holiday – not only can you loot his house but you can use the familiarity exploit rouse and call his work claiming you are working with him on something urgent and request information. Depending on the quality of data protection policies in place you might be able to access something confidential through one of Bob's colleagues.

- **New technology** – it is now easier to fake identity cards. There are also all sorts of tiny cameras and microphones on the market which help the social engineer gather information.

- **Services** – any service that involves geo-tagging will tell a social engineer where you are if they can tap into it. There are also very unethical telephone call centre services available who will masquerade as someone on your behalf. Picture the scene – you have stolen a credit card from an elderly lady and you want to purchase expensive items with it. To achieve this you want to change the billing address for the credit card. Problem – you are not an elderly lady, nor you can mimic one, so calling the bank yourself is out of the question.

If you don't have a friend who can call for you, you can actually purchase the service. Believe it or not, there are companies out there that will charge you around \$7-15 to make the call to the bank on your behalf if you provide them with enough information to pass the security questions.

Risky business - am I at risk?

Yes! Everyone is at risk of being targeted by a social engineer. Even if a social engineer doesn't think they can get access to you directly, they may try to target you through your friends, family, or colleagues. For example, they may hack into your friends' email account and send a message inviting you to click on a link. Because you trust your friend, you are more likely to click the link.

Tips for reducing risk

From a personal perspective, probably the most useful piece of advice is an oldie but

goodie: "If it sounds too good to be true, it probably is". Also, if you are unsure about the authenticity of an email or a letter, use contact information you have sourced independently (rather than that provided) to verify it.

As an employee of a company, you need to ensure that you are not exploited to give away trade secrets. In this instance, increasing your knowledge of how social engineers operate and adopting a questioning nature will help – i.e. if someone you don't really know asks you something confidential, don't be afraid to challenge them.

If in doubt, seek confirmation that you can share the information with that person from a trusted source before proceeding. Also, follow the data protection policy – e.g. if you have been told not to access personal email at work, don't just assume your employer is being unreasonable, because there may be a very good reason for the policy.

THE MOST USEFUL PIECE OF ADVICE IS AN OLDIE BUT GOODIE: "IF IT SOUNDS TOO GOOD TO BE TRUE, IT PROBABLY IS".

As an employer or business, remember that it is all good and well to spend money on technical protection systems, but if you don't train your staff to avoid social engineering attempts and teach them good data protection practices, your system is still vulnerable. It is important to explain to staff why you have certain policies in place. For example, if you block access to personal email accounts to help minimize the risk of malware being downloaded, then inform staff about this rationale.

You might also want to consider adopting the "least privilege" principle, which means providing users with access only to specific places - basically, the need-to-know translated into a need-to-access.

The bottom line is that if the person cannot access the system, they cannot abuse it (either intentionally or unintentionally). I have been subject to this myself and actually found

it reassuring as it meant I couldn't accidentally break anything!

You might also want to employ penetration testers who can test the effectiveness of your security procedures by trying to socially engineer their way into your business. They can test whichever security measures you want and will report back with recommendations for improvement.

Penetration tests can be physical (e.g. someone trying to get past building security) or through the IT systems (e.g. white hat hackers will attempt to breach your IT security systems). For more information on white hat hacking, search online for Archangel, also known as "the Greatest Social Engineer of All Time", to see how successful this approach can be. One word of advice, don't warn your staff that a penetration tester is coming – it undermines the whole operation!

Predictions

Social engineering will never go away. In fact, the more technologically advanced we become, the more necessary it is to use social engineering to gain access to IT systems. The methods are unlikely to change – social engineers have been using the same basic tricks (e.g. familiarity exploits) for years and there is no reason for them to change now.

The only difference is that new technology provides different ways of achieving their aim (e.g. allowing them to improve or automate their attacks). Secondly, social engineering

attacks are likely to continue to become more sophisticated and targeted.

As people become more aware of social engineering tactics, it is necessary for them to up their game to ensure continued success (e.g. the development and use of social engineering services).

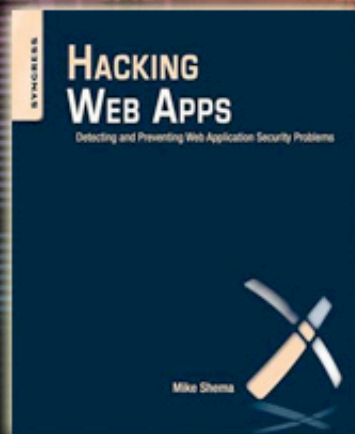
Finally, remember the birth of social media has acted as an enabler to social engineering, so be careful what you post. In summary, remember that an easy target creates easy information and you are only as strong as your weakest link.

Dr. Amy Burrell holds a BSc in Applied Psychology, an MSc in Forensic Behavioural Science, and has recently completed a PhD in Psychology. Amy is a Training Manager at Perpetuity Training, a company specializing in security and risk management training. As part of her role at Perpetuity, Amy is a tutor for students on the Security Institute distance learning programme, and also lectures on BTEC short courses and supports the development of bespoke training courses. Find out more about Amy and the work she does go to www.perpetuitytraining.com or email training@perpetuitytraining.com

FRESH SECURITY NEWS

www.twitter.com/helpnetsecurity

twitter



Review: Hacking Web Apps

by Zeljka Zorz

Web security impacts applications, servers and browsers. Successful attacks against Web applications and sites means bad news for their owners, developers and users.

This book explains the ins and outs of eight types of security weaknesses and flaws most commonly exploited by hackers, and advises on how to fix them.

About the author

Mike Shema develops web application security solutions at Qualys. His current work is focused on an automated web assessment service, but his security background ranges from network penetration testing, wireless security, code review, and web security.

Inside the book

The book rightfully starts with a comprehensive chapter on HTML5. As this latest version of the language on which the entire Web is based slowly moves towards becoming the de facto standard, it will simplify the life of web developers as well as provide more guidance on security practices and stricter rules for HTML parsing. The author has done a good job explaining the adopted changes and point-

ing out the security considerations web developers should think about in order to avoid implementation errors.

The topic of HTML injection and cross-site scripting (XSS) attacks is addressed next: how they are executed, why they are so prevalent and still so difficult to defeat, and what to do to protect your web resources and its visitors from them.

The third chapter deals with Cross-Site Request Forgery (CSRF) attacks, during which hackers take advantage of the users' already established relationship with a site, "impersonate" them, and execute fraudulent transactions, "steal" their clicks, and more.

SQL injection and data store manipulation attacks have been tackled in the fourth chapter. Even though it's easy to apply countermeasures against SQL injections, we still keep hearing how websites and databases get compromised with this type of attacks.

The author beautifully explains why that is still happening, and what to do about it, making this a chapter that every web developer should know by heart.

The same can be said about the following chapter about attacks aimed at breaking authentication schemes (mainly password authentication) - session token replaying or reverse engineering, brute forcing, sniffing, and others. Here you can brush up on some of your encryption knowledge, as well as learn about a number of alternate authentication frameworks such as OAuth 2.0 or OpenID.

The last two chapters deal with design deficiencies' abuse, logic attacks, application, system and network weaknesses and how they are usually exploited.

The final chapter addresses browser and privacy attacks, and teaches about how malware attacks browsers and how you can better protect your privacy and data online. Recommended countermeasures are a mix of advice on setting configuration, online browsing behavior, and recommendations of various online services and plugins, and this last part

could definitely be of use to every Internet user.

Throughout the book the author adds handy tips and "Epic Fail" stories that help draw the readers' attention to potential mistakes and drive home certain points that are best to be remembered.

Final thoughts

This relatively short book is a perfect fit for budding and active web developers, but not so much for everyday Internet users. Readers who don't know the first thing about HTML, JavaScript, and in general how the Web "works" will be struggling to keep pace.

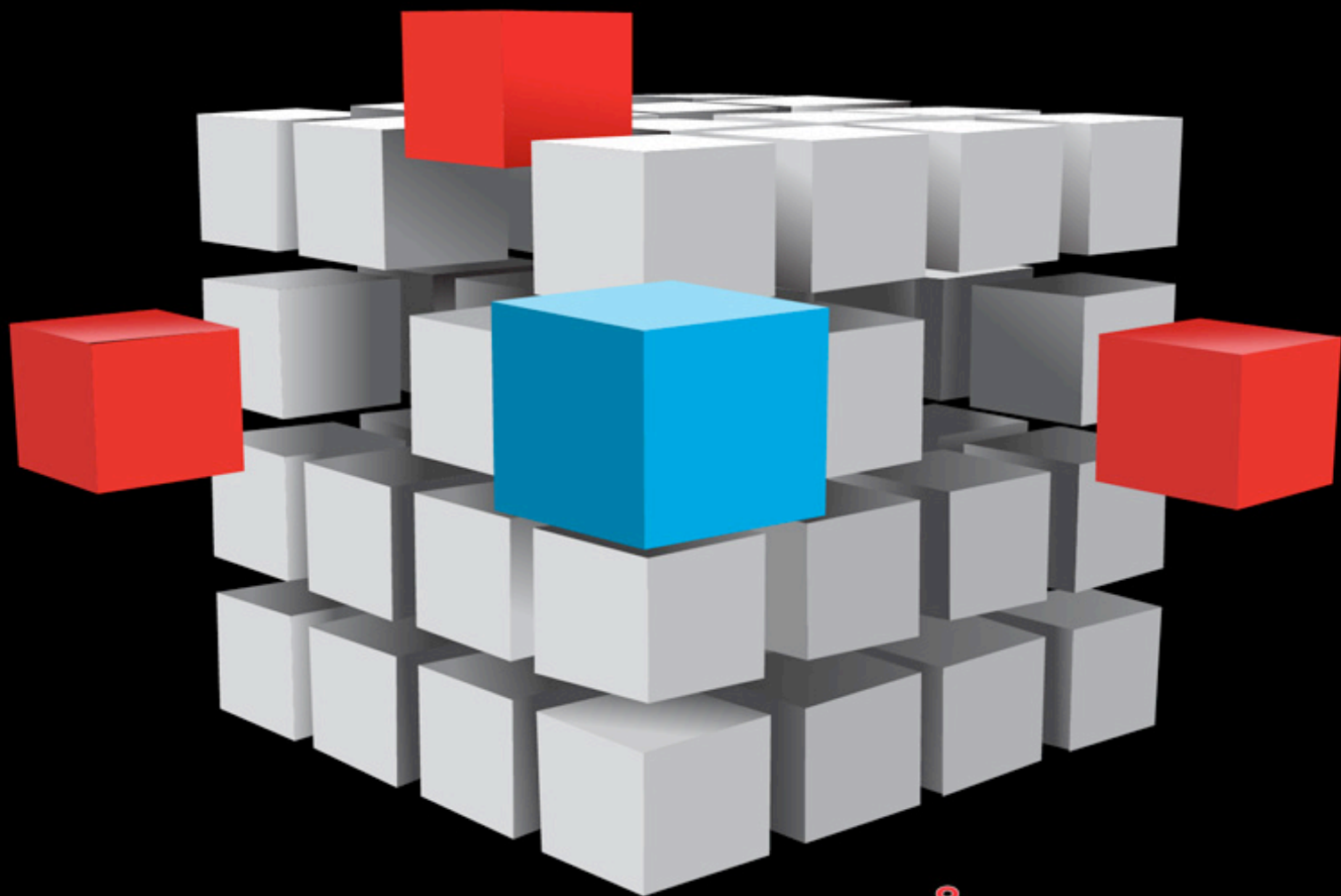
I found this book to be a great source of information and very easy to read. The author explained the subject matter well, and stopped (perfectly) short of delving into the minute technical intricacies.

Given the effectiveness of the attacks addressed in the book, I should think that even seasoned web developers might want to consider taking a peek and see if they had been ignoring some of the things in it.

Zeljka Zorz is the Managing Editor of (IN)SECURE Magazine and Help Net Security.



HITBSECCONF2013



amsterdam

April 8th - 11th 2013 @ Hotel Okura

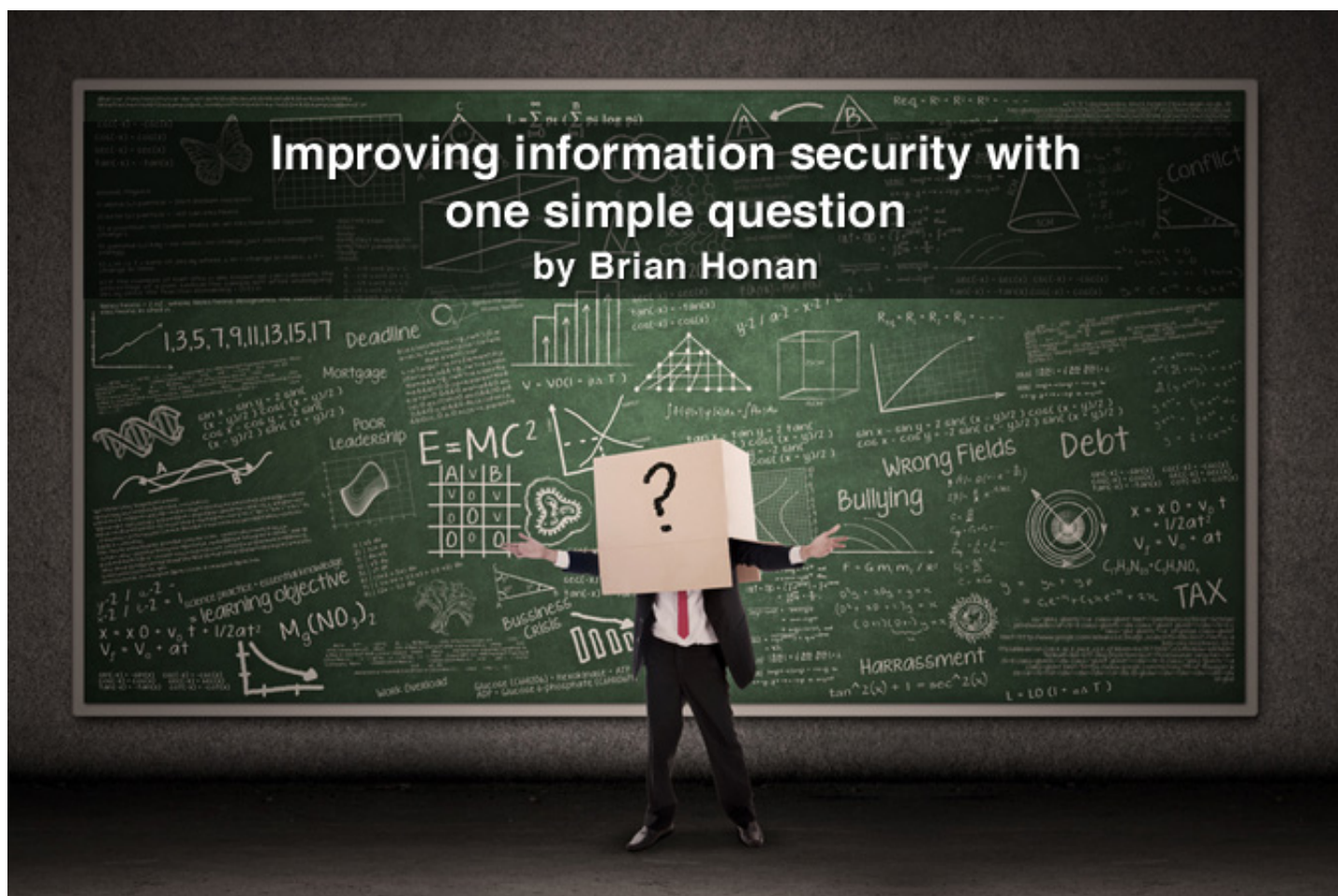
REGISTER ONLINE

<http://conference.hitb.org/hitbsecconf2013ams/>

THE FOURTH ANNUAL HITB SECURITY CONFERENCE IN EUROPE
WITH KEYNOTES BY:

EDWARD SCHWARTZ (Chief Information Security Officer, RSA)

BOB LORD (Director of Information Security, Twitter)



Anyone who has children, or has had to deal with very young children, will understand how powerful the word “why” is and how it can drive their curiosity. Innocent-sounding questions such as “why is the sky blue?” can lead to the question “but why?” to each of the answers given. A cycle of never ending “whys” is quite commonplace until it seems all the answers have been exhausted, but still they will ask “why?”

This small and seemingly innocuous word can also be one of the most powerful tools in the vocabulary of the information security professional.

Those same three letters that drive many parents crazy were also the driving force for many of the early pioneers in information security. Their curiosity and wondering “why?” led these pioneers to experiment, to poke, to examine, and to learn as much as they could about the computer systems, the networks, and the applications they used. This knowledge was then used to further improve those systems and today our interconnected world is a result of those people asking that simple question.

I believe that an inherent curiosity is one of the key traits every successful information security professional should have. That sense of

wonder and seeking to find out why things work in a certain way, many times by breaking them, is what makes this profession such an exciting and interesting one.

Unfortunately, I have noticed recently that many people are no longer seeking to find out why things work in a certain way. We seem to have moved to an industry that is too willing to accept how things are presented to us without challenging it. We focus on compliance issues, react to media stories, listen to speakers at conferences, or swallow all the material that vendors pitch our way.

Instead of asking why, we are now asking who, what, where or when. Instead of asking “why do I need to be compliant with a certain standard?” we are asking “what do I need to do in order to be compliant?” Instead of asking “whom should I allow to have their device

access the network” we need to be asking “why am I allowing access?” When vendors pitch their solutions to us we need to stop asking “what is the solution? Or indeed what is the problem?” and instead ask “why do I need this product?” For each answer to these questions we should continue to ask “why?” until we have exhausted all avenues of questioning and have a fuller and better understanding of the issues we are trying to address.

While the “what?”, the “who?” and other such questions are important, they do not get to the core of how best to secure our systems and data. It is the “why?” that drives the curiosity

of the 4 year old child, and the “why?” should drive our need to better understand, too. Asking this question not only leads us to discover the reasons we need to do things, but it also helps us to examine the motives behind the headlines and stories that we read.

We see an ever increasing number of news stories about the threat of cyber-war, the need for cyber-warriors and cyber-weapons, the rise of the Advanced Persistent Threat (APT), the risks that Bring Your Own Device raises, and the security issues with Cloud computing. If we simply consume these stories without asking “why?”, we may never learn to understand the motives of those behind the story.

By engaging with our business colleagues and asking them the question “why?” we can better understand the issues the business is trying to address.

Why are vendors pitching story after story about the above issues? Is there a genuine concern that we should be aware of, or is it simply a way for vendors to make companies more nervous about their security and therefore buy their products?

Is all the talk and hype about cyber-warfare and cyber-weapons something that we all should worry about or is it a way for vendors and other interested parties to create a perceived need for governments and industry to provide funding in this area? By asking “why are these stories appearing in the first place?” we can better understand the issues that really affect us as professionals, as a community and also affect our organizations.

The question “why?” should not just be reserved for vendors, pundits and those in the

information security industry - we should also look into our organizations and ask the same question of them. We need to better understand the business that our organizations are conducting so we can better protect them.

By engaging with our business colleagues and asking them the question “why?” we can better understand the issues the business is trying to address. It can help us eliminate unnecessary distractions and allow us focus on delivering real value and benefits to the organization.

Let’s stop being distracted by the “who?”, the “what?”, the “where?” and the “when?”. Let’s focus instead on the “why?”. It is time to reignite the curiosity that drove the early pioneers of the security community and made “why?” a useful tool once again.

Brian Honan is an independent security consultant (www.bhconsulting.ie) based in Dublin, Ireland, and is the founder and head of IRISCERT which is Ireland's first CERT. He is adjunct lecturer on Information Security in University College Dublin and he sits on the Technical Advisory Board for a number of innovative information security companies. He has addressed a number of major conferences such as RSA Europe, BruCON, IDC and Source Barcelona and numerous others. Brian is author of the book "ISO 27001 in a Windows Environment" and co-author of "The Cloud Security Rules".



HITBSecConf2013 - Amsterdam

www.conference.hitb.org

Okura Hotel, Amsterdam, The Netherlands

8 April-11 April 2013

InfoSec World Conference & Expo 2013

www.misti.com/infosecworld

Walt Disney World Swan and Dolphin, Orlando, FL, USA

15 April-17 April 2013

Infosecurity Europe 2013

www.bit.ly/ZtvPhp

Earls Court, London, UK

23 April-25 April 2013



Why do you need a policy or governance? Well, it is common sense that security needs to be handled at the very top of any organization.

The reasons for that simply are that first, security collides with business (it costs money, it increases the burden, it is inconvenient), second, only the top management can make the decision about the trade-off between a secure organization and an insecure one, and third, only top management can take the associated risks.

A policy is a written, approved and signed document by the executive(s) and contains and states their commitment and intended directions on where the company shall go and what they see as appropriate dealing with the issue.

It is clear that only if those executives live up to their own statements and policies (“do what you say”) the policy will over time bear a fruit and change employees' perceptions. If lower rank employees see that executive management demands (and approves for himself) exceptions or circumvents / breaches policy, the herd will follow that behavior.

Since the governance of security can be quite complex, it is best practice to split the overall policy into a pyramid of documents, where the highest level document is the “Security Policy” and the lower level documents (standards, procedures, and to some extent guidelines) form a more and more detailed and explicit description of how things are to be done.

The security policy makes clear statements of “why” something shall be done, and what direction is to be taken. The security standard documents will focus on the “what” shall be done and clarify and set clear standards for what must be done.

The procedure level documents will explicitly show “how” the “what” is to be implemented step by step. Finally, some guidelines may be necessary as long as standards and procedures don’t exist, but they certainly will not have the same weight as a standard – as they are more seen as guide (should / may) than as direction (shall / must).

Guidelines can be useful in situations of ambiguity or which are yet uncovered by other documents, and at least you can provide some kind of directions for the implementers. However, do try to avoid the guideline approach as much as possible.

Get policies, standards and procedures in place instead – this serves your company much better and will enable the administrators and other technical staff to implement security throughout the environment.

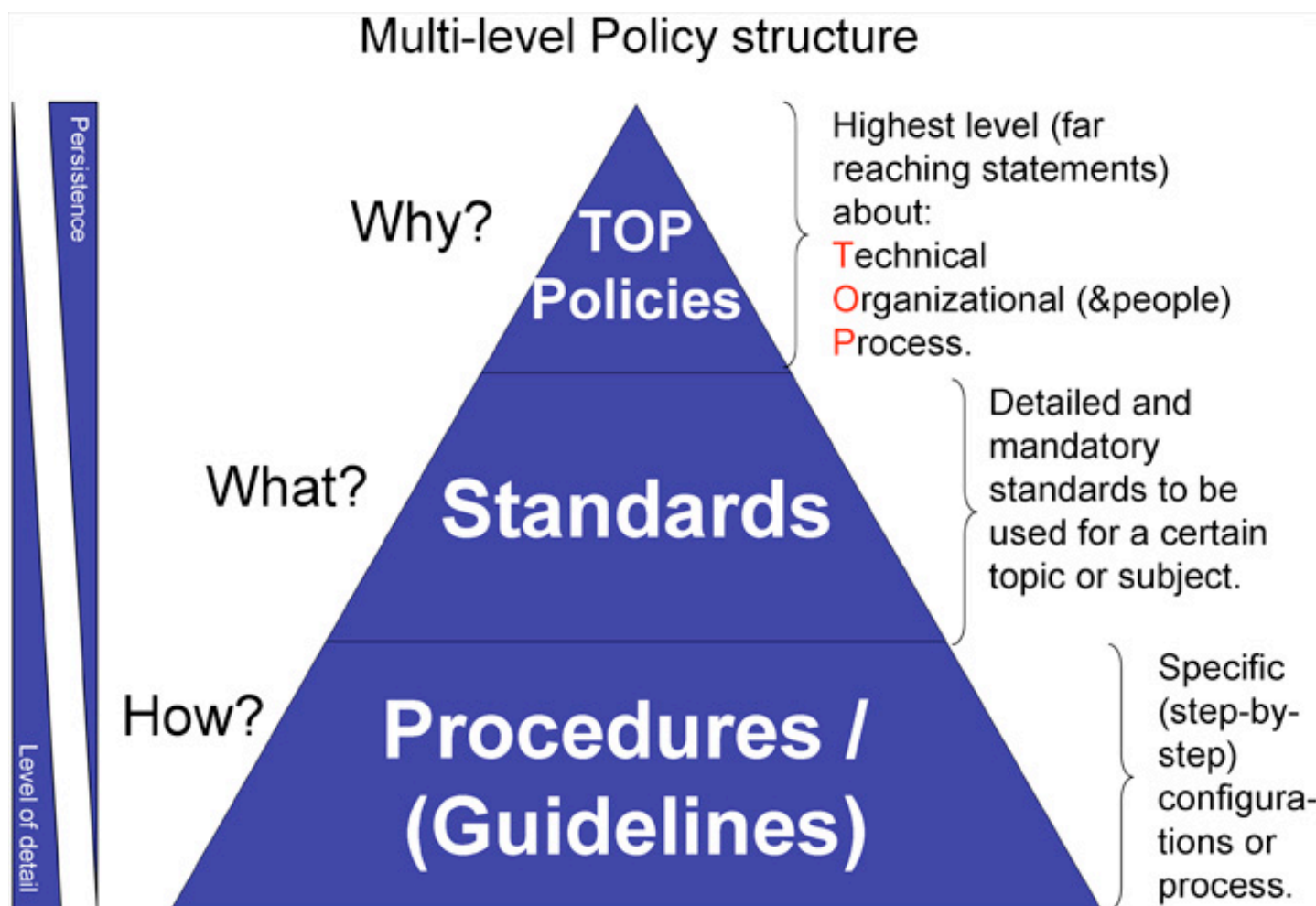


Figure 1: Multi-level policy structure.

Here is an example: let's assume your company executives consider that a loss of a mobile device with information on it could be a huge risk (be it bad press, loss of customer trust, actual fines /penalties by regulatory oversight bodies, and the like). They might state in the policy a sentence like this:

"All information classified and marked as 'confidential' must be at all times secured as defined in the security standards and procedures against access, modification or destruction by unauthorized parties".

From a security perspective, this is a pretty good statement, provided that a clear classification document is in place which handles the

definition and security standards of "confidential" or "sensitive" information. Just to complete this level of security documents, here is a much worse example of that same sentence:

"Sensitive information should be reasonably protected".

Well, this speaks volumes of the executives who signed off on that. What does "sensitive" mean? What is reasonably? They leave this up to the reader to interpret and it is unclear if they will back it should a situation of conflict appear. Do you see the difference in clarity? To be clear, I don't agree with the commonly taken approach that the top level policy

just should state “take care for the confidentiality, integrity and availability of our data”. This will not help and it sets the wrong “tone” at the top. Executives need to be concise and clearly convey their commitment and expectations.

Now let’s get one level deeper in the above policy example and describe how the standard document could read like this:

“At XYZ Corporation we classify our information as outlined in the ‘data classification policy document’ and follow the (following...) processes and procedures to always handle the data accordingly. Information labeled as “confidential” must be encrypted both at rest and in transit using the AES-256 security algorithm. In the case that certificates using public key encryption are being used, a comparable quality of key length (i.e. 2048 bit, elliptic curve or prime factor algorithm for the key exchange) must be used instead. Should these algorithms need to be changed due to technical advances or breach, the appropriate standards will be described in this document. It is imperative that data at rest (i.e. hard drives) will be encrypted in full (full disk encryption instead of partial file encryption) and that data in transit will be encrypted end-to-end (data end points, i.e. client-server or server-server), leaving no way to attack in between. The specific solution for the full disk encryption is product ABC and the installation and configuration steps are documented and to be followed in the procedure level document of this security standard (...). For the data in transit, the following solutions are to be used, based on the use-cases (...). Information labeled with “high integrity” needs will be hashed in the following ways (...). Information labeled as “high availability need” will be served in the (redundant) data centers and backed up online with the following procedures (...).”

Hence, we have detailed and specifically clarified the overall security policy without changing its original intention or direction. Please understand that the uses (...) need to

be outlined, depending on your company’s situation – I just want to focus on the overall story here.

In the procedures level document of the information security policy, you need to define a step by step approach to how the standard document will be implemented. Example:

“As directed by the security policy and standard documents (...) XYZ Corporation uses the product ABC to provide for full disk encryption. For servers (/for clients...) the currently licensed version is 1.2.3 and the installation files are here (...). Before installing this product please verify the licenses are in order. The product is to be installed in the partition UVW in the following path (...). It consumes X bytes and needs the following configuration settings (screenshots, detailed instructions follow)...”

The procedure document is clearly labeled as such with a date, versioning information, author and document ownership assigned. It is accessible by the authorized people in IT only and needs to be shredded once out of life. This is to prevent giving outside attackers an opportunity to find a weak setting just by dumpster diving.

I hope these examples make it clear why the multi-level policy approach is the best practice, and how one can easily achieve this. To save space I have not included detailed screen shots and further configuration information in the above example procedure level document, but it should be clear by now that this will be the most descriptive and specified document (“the thickest book”) of all above mentioned levels.

The guidelines could read similar to the above standard – but they will lack the imperative and will always provide options and possible solutions without making the application of it a mandatory action. I do not intend to give an example here. The provided examples of a policy statement, standards formulation, and procedure level content will help the technical people (those who technically “enforce” the paper statements and executive directions) to do what is expected, and also these signed

and approved policies will help them against the so called “screaming Vice President”.

The combination of both well written and technically implemented policies will serve the intended protection level long-term and will form an important part of the needed governance.

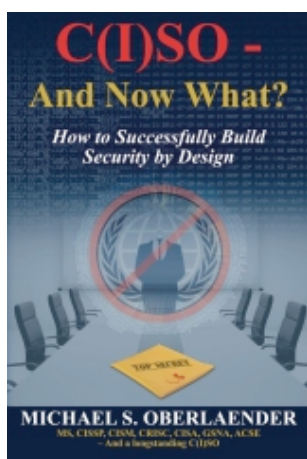
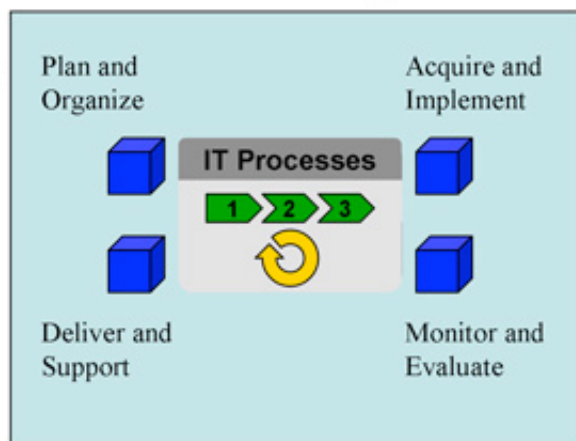
Other points of governance are the required processes, and especially the change-management processes in place. ITIL (v3) is the generally accepted industry standard for this and it should be very clear by now, that no port will be opened up without a written change management clearance and proper management (that means, all involved parties,

the system owner, the data owner, the business side, the chain of command) approval – this is just one example and holds true for any change to the production environment. Also, any change to the production environment should first be tested in the test environment, and if you don't have one, get one installed (and required by policy).

Governance is of course more than that; the COBIT (Control Objectives for Information and related Technology) standard with its 34 processes shown in the picture below provides a pretty well rounded description and should be used for orientation and implementation over time. I have marked the ones in red with a direct impact on security:

COBIT – 34 processes compact

P01 Define a Strategic Information Technology Plan	DS 1 Define Service Levels
P02 Define the Information Architecture	DS 2 Manage Third-Party Services
P03 Determine the Technological Direction	DS 3 Manage Performance and Capacity
P04 Define the IT Organization and Relationships	DS 4 Ensure Continuous Service
P05 Manage the Investment in Information Technology	DS 5 Ensure Systems Security
P06 Communicate Management Aims and Direction	DS 6 Identify and Attribute Costs
P07 Manage Human Resources	DS 7 Educate and Train Users
P08 Ensure Compliance with External Requirements	DS 8 Assist and Advise IT Customers
P09 Assess Risks	DS 9 Manage the Configuration
P010 Manage Projects	DS 10 Manage Problems and Incidents
P011 Manage Quality	DS 11 Manage Data
	DS 12 Manage Facilities
	DS 13 Manage Operations
A11 Identify Solutions	M1 Monitoring the Processes
A12 Acquire and Maintain Application Software	M2 Assess Internal Control Adequacy
A13 Acquire and Maintain Technology Architecture	M3 Obtain Independent Assurance
A14 Develop and Maintain IT Procedures	M4 Provide for Independent Audit
A15 Install and Accredite Systems	
A16 Manage Changes	



Michael S. Oberlaender is a world-renowned security executive, thought leader, author and subject matter expert and has worked in executive level security roles (CSO/CISO) both in the US and Germany, and in IT for over two decades. Most recently he has been serving as Chief Security Officer for the largest European cable network provider in Germany and before served as Chief Information Security Officer for FMC Technologies Inc, an oil field services and engineering company in Houston, TX.

He is the author of "C(I)SO - And Now What?: How to Successfully Build Security by Design" (ISBN: 978-1480237414), which covers your initial phases in the job such as setting expectations, base lining, gap analysis, capabilities building, and org chart variances. It then leads you to define security architecture, addressing a secure development process, application security and also security policy levels. Further items such as awareness programs, asset

management, teaming up with audit, risk management, and finally the strategy development are covered. Then we dive into ROIs, trust relationships, KPIs, incident response, forensics, before we run into crises management by looking at some specific examples of personal experience of the author - himself a C(I)SO for many years. The book is ending by providing advice how to deal with other executive management, and what kind of education, certifications, and networking you need to focus on.



8 key data privacy considerations when moving servers to the public cloud

by Steve Pate

The interest in Infrastructure as a Service (IaaS) is clearly growing. In fact, Gartner recently reported that IaaS is the fastest growing segment of cloud services, at a rate of 45% in 2012.

The reasons are well understood: cost savings, improved elasticity and scalability, along with ease of deployment. However, organizations must also consider the security of their data when they move operations to the public cloud. Here are eight considerations you should not overlook before you make your move.

Encrypt your data

Good security must be done in layers, and there is no single mechanism or tool that will give you absolute security. Ensuring data privacy in the cloud is no different. However, many organizations start by building external defenses, when in many cases it's easier to start with what you are trying to protect in the first place – the data.

If the default state of the data is secure, then it becomes easier to control, monitor and protect access to it. Think of encryption as a foundation for your presence in the cloud.

Proper encryption is a great way to solidify your data, and it's a start, but there are still many more layers to go.

Retain exclusive control of your keys

Encrypted data is only as secure as the method used for handling the encryption keys. We all understand the folly of locking your house and then placing the key under the doormat, and you certainly wouldn't hand that key to someone you don't know. Instead, you keep your keys close by so that you (and only you) have access. Similarly, when you run applications or put encrypted data in the cloud, make sure you control your encryption keys. Many cloud providers offer some form of encrypted storage — but they retain possession of keys. The best solution is to retain control of key storage either in your private data center or with a service in the cloud that is entirely separate from the cloud service provider holding your data.

Avoid platform and vendor lock-in

OK. So you've made the decision to encrypt your data and ensure you control your keys. That's great! But, you're not done yet; if the mechanics of your encryption solution are bound to a specific virtualization platform or a specific cloud service provider, you're painting yourself into a corner.

One of the reasons you are in the cloud is so you don't need to own the infrastructure. Instead, you rent it as needed. Adopting an encryption solution that ties you to a specific provider's infrastructure can reduce your ability to move to where you get the best service and support.

Make sure that you have secure multi-tenancy

In the public cloud, different companies share the available resources and the importance of multi-tenant practices becomes even clearer. Cloud providers will do their job: they will move our VMs (virtual machines) between machines, replicate their images and create multiple backups so they can provide us with the robustness and performance we demand.

This means the files of different organizations are copied many times, and co-mingled across multiple storage, backup and other devices. Cryptographic separation of my applications and data from yours lets all of us operate securely in this shared environment.

Require more than one key

All encryption is not created equal. There are flavors of storage encryption that require only a single "customer" key and there are others that require only one key for a physical device.

These methods are weak at best; at worst, they cause a significant problem if you need to securely decommission a VM or rekey its data. When you are placing multiple virtual machines in the care of a cloud provider, you want at least one key per VM. Yet, the more likely scenario is using individual keys for each virtual disk that a VM uses to store its data.

The good news is that this problem that has already been solved. There are encrypting solutions that allow you to manage separate keys for your VMs so that you always have individual keys per VM or virtual disk. This gives you the granularity of control you need without adding undue complexity.

Make sure that you can get your data out of the cloud

Putting your data into the cloud is becoming easier every day. Creating a VM to host an application can literally be done in minutes with a provider like Amazon, which gives you fantastic flexibility and scalability. However, what happens when you want to pull that application out of the cloud, retire the data, or even delete it entirely? Good luck.

The best way to ensure that you can securely decommission data in the cloud is by keeping it encrypted and working with a key management system that lets you shred the keys, if and when that time comes.

Address regulatory requirements

There is an ever-increasing body of laws, rules and guidelines concerning how you must handle sensitive data. For example, the regulations for the Payment Card Industry Data Security Standard (PCI DSS) are there to guarantee your credit card data is kept secure when handled by vendors, banks and all other processing partners that have a relationship with your data.

The regulations are constantly being updated as technology changes. Whether they are the new PCI DSS virtualization guidelines published in February 2013 or the HIPAA/HITECH regulations in place, the simple fact is that any data that must be kept private should be encrypted, and it's easier than ever to make this happen.

Archaic, expensive systems that encrypt only specific data are giving way to cost-effective, effortlessly deployable solutions that encrypt data, applications and systems more broadly.

Gain safe harbor from breach notification laws

There is a specific exemption written into 47 of the 51 laws on the books. That exemption is a “Safe Harbor” clause for encrypted data and where the keys have not been compromised.

The law says that if you do not encrypt your customer’s data, or if you fail to properly protect the encryption keys, then a data breach will potentially subject your organization to public damage to its reputation as well as expose you to civil (and potentially criminal) penalties. A federal law on this matter will likely pass in the U.S. Congress at some point this year that will codify this for all of the United States.

It could not be clearer. Any business running applications that handle customer data in the cloud should encrypt that data and should manage their keys securely and separately from the cloud provider holding that data.

Conclusion

In short, a security strategy with a multi-pronged approach can certify you make a safe leap to the cloud, and will allow your organization to take advantage of all the benefits it offers.

Encryption should be a critical component of your strategy – but make sure that the solution you choose offers the flexibility, control and scalability you’ll need in the cloud.

Steve Pate is co-founder and CTO at HighCloud Security (www.highcloudsecurity.com), a startup providing solutions to help customers protect their virtual machines both in the data center and in the cloud.





Top 10 things that all organizations need to audit... but often don't

Ask an IT manager to tell you **who** changed **what**, **when** and **where** in an IT infrastructure and it will often involve a time-consuming manual process of trawling through a disparate array of native audit logs from servers and network equipment. Despite being slow and insecure this manual approach is still common-place even in the largest of organizations.

In reality very few IT teams know what is happening in their infrastructures at any one time. With increasingly complex IT infrastructures, there is a lot to keep track of but below is the checklist of top 10 things companies really should be auditing:

- | | |
|--|---|
| <input checked="" type="checkbox"/> Active Directory | <input checked="" type="checkbox"/> System Center VMM |
| <input checked="" type="checkbox"/> Exchange | <input checked="" type="checkbox"/> Windows Server |
| <input checked="" type="checkbox"/> VMware | <input checked="" type="checkbox"/> Network Devices |
| <input checked="" type="checkbox"/> EMC Celerra/VNX | <input checked="" type="checkbox"/> SQL Server |
| <input checked="" type="checkbox"/> NetApp Filer | <input checked="" type="checkbox"/> SharePoint |

"We needed to comply with global auditing standards, and were instructed by our auditors to find a solution that met their exact requirements. NetWrix's Change Reporter Suite allowed us to monitor all critical aspects of our Microsoft environment, thus meeting the auditors' strict requirements"

Mervyn Govender, CIO, CreditEdge

Although native auditing tools are capable of detecting that something has been changed in an IT environment they lack auditing capabilities to provide the elaborate information on every single change that has occurred in any system from a top 10 list – for example, who deleted an organizational unit in Active Directory, who created a new virtual machine, who accessed sensitive files or file servers, who deactivated strong password policy, what servers were removed from SharePoint, etc.

NetWrix Change Reporter Suite

NetWrix Change Reporter Suite automates and simplifies the auditing of critical IT systems across the entire IT infrastructure. With one simple deployment you can efficiently audit critical IT systems such as Active Directory, Exchange, VMware to name just a few - while staying within a reasonable budget.

Unlike traditional log management solutions, NetWrix Change Reporter Suite makes it very easy to find relevant answers to key questions: **who** changed **what**, **when** and **where**, including "before" and "after" values for modified settings. The product streamlines compliance to HIPAA, SOX, PCI, GLBA, FISMA and many other regulations, provides an easy-to-use solution that drastically improves IT infrastructure visibility and internal security.

Download FREE Trial:
netwrix.com/trial

